PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Programa de Pós-Graduação em Relações Internacionais

Eduardo Kraemer Góes

A *ESPADA DE MÚLTIPLOS PROPÓSITOS* DA COREIA DO NORTE E OS CRIMES CIBERNÉTICOS

O impacto na balança de poder

Belo Horizonte
2025

Eduardo Kraemer Góes

A *ESPADA DE MÚLTIPLOS PROPÓSITOS* DA COREIA DO NORTE E OS CRIMES CIBERNÉTICOS

O impacto na balança de poder

Tese apresentada ao Programa de Pós-Graduação em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Doutor em Relações Internacionais.

Orientador: Prof. Dr. Eugênio Pacelli Lazzarotti Diniz Costa

Área de Concentração: Política Internacional: Instituições, Conflitos e Desigualdades

Belo Horizonte
2025

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Góes, Eduardo Kraemer
G598e A espada de múltiplos propósitos da Coreia do Norte e os crimes cibernéticos: o impacto na balança de poder / Eduardo Kraemer Góes. Belo Horizonte, 2025.
177 f. : il.

Orientador: Eugênio Pacelli Lazzarotti Diniz Costa

Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais

1. Tecnologia da informação e da comunicação. 2. Segurança da informação. 3. Segurança de dados. 4. Cibercrime - Coréia (Norte). 5. Poder (ciências sociais). 6. Coréia (Norte) - Relações exteriores. I. Costa, Eugênio Pacelli Lazzarotti Diniz. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais. III. Título.

CDU: 355.02
Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB6/2086

Eduardo Kraemer Góes

A ESPADA DE MÚLTIPLOS PROPÓSITOS DA COREIA DO NORTE E OS CRIMES CIBERNÉTICOS
O impacto na balança de poder

Tese apresentada ao Programa de Pós-Graduação em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para obtenção do título de Doutor em Relações Internacionais.

Área de Concentração: Política Internacional: Instituições, Conflitos e Desigualdades

---

Prof. Dr. Eugênio Pacelli Lazzarotti Diniz Costa – PUC/MG

Profa. Dra. Raquel de Bessa Gontijo de Oliveira – PUC/MG

Prof. Dr. Jorge Mascarenhas Lasmar – PUC/MG

Profa. Dra. Danielle Jacon Ayres Brito – UFSC

Profa. Dra. Graciela de Conti Pagliari – UFSC

Belo Horizonte, 24 de fevereiro de 2025.

AGRADECIMENTOS

> "Digo: o real não está na saída nem na chegada: ele se dispõe para a gente é no meio da travessia." – Guimarães Rosa (Grande Sertão: Veredas, 1956)

> "Se aprendesse qualquer coisa, necessitaria aprender mais, e nunca ficaria satisfeito." – Graciliano Ramos (Vidas Secas, 1938)

Então é assim que a gente sente quando se termina um Doutorado? A mim, parece-me o fim de uma aventura e de um ciclo de dúvidas, só para chegar num outro, com mais dúvidas.

Para trilhar esse caminho, tive o apoio de muitos. É clichê dizer: "não foi fácil". Mas realmente não foi. Frequentar as aulas, aprender com professores magníficos, mesmo com quem tive contato em uma só aula, e conciliar com o trabalho profissional sem diminuir a qualidade não foi fácil. Também não foi fácil a vida pessoal: no meio do caminho houve uma pandemia. Sim, houve uma pandemia no meio do caminho! Felizmente passei por ela, assim como os meus.

No meio do caminho apareceu também uma Patrícia. Surgiu uma Patrícia no meio do caminho. Mas ela não foi pedra, nem obstáculo. Ela foi meu suporte em diversos momentos, meu puxão de orelha, meu socorro. Não à toa, casamo-nos durante o processo. Obrigado por tudo, Linda. Te amo! Nina, não sinta ciúmes, também amo você" Obrigado por me aceitar e apoiar.

Meus pais, João Eduardo e Suzana, e meus irmãos, Carol e André, torceram da forma como podiam e tenho certeza de que, se precisasse, estariam prontos para ajudar no que eu precisasse. Muito obrigado! Amo vocês.

Boris, Guto, Nego, Pandora, Gata, Tom, Flor, Fred, Cop, Miau, Mel, Zezinho e Marta, vocês me fazem um humano melhor. Também me deram apoio, às vezes até demais! Muito obrigado!

Ao pessoal do McArrão: Hugo, Lobão, Eric, Leo, Pedro, Guimarães, Breno, Suzy, Pãozinho, Joyce, Débora, Ju, Ana Paula, não necessariamente nessa ordem, isso aqui tem um pouquinho de cada um de vocês. Valeu demais pela companhia, sempre.

Felipe "Husky", você quem me chamou primeiro a atenção para muitas coisas nas Relações Internacionais, e nem imagina o quanto me ensinou. Você é um dos principais culpados por esse trabalho. Muito obrigado!

Ao professor Eugênio pelos ensinamentos, acolhimento, paciência e conversas, meu imenso muito obrigado!

Aos colegas e (ex-)alunos da PUC-MG, especialmente Andréa Resende, Bruno Maciel, Gustavo Dall'Agnol, Dudu Maia, Pedro Rocha, Rafaela Sanches, Bruno Haeming, Carolinna Maria, Aimara, Fabiana Sander, Leonardo e Rafael, não consigo dizer o quanto nossas

conversas foram produtivas, me trouxeram muito conhecimento e fizeram-me crescer como pessoa. Não poderia deixar de citar os amigos Christian Azevedo e Guilherme Damasceno, colegas de pós-graduação e de trabalho. Considero vocês todos meus professores e sou-lhes muito grato. O isolamento pela pandemia e a falta dos encontros na PUC-MG fizeram-me muita falta.

Aos componentes da banca, com seus comentários e orientações, meu muito obrigado pela dedicação na leitura e por ajudar a enriquecê-lo.

Andréa, Adriane, Joana, Rodrigo, Leo e professora Cris, o apoio extra tese de vocês foi essencial todos esses anos. Muito obrigado!

Ao Setor Técnico-Científico da Superintendência Regional da Polícia Federal em Minas Gerais, obrigado pelo apoio quando precisei. Agradeço especialmente a vocês, Alexander, Marcus Vinícius, Parma, Soares, Wenderson, João Luiz, Verçosa, Soares, Bruno, Queiroz, Rodrigo, Zocrato, Carlos, Maurício, Mauro, Macedo, Guilherme, Scarpelli, Clemente, Lemos, Eduardo... É gente demais, sô! Ainda, Peixinho, Meiga, Toledo, De Nardin, Guilherme e Laplace, obrigado!

Ao corpo de funcionários do Programa de Pós-Graduação em Relações Internacionais da PUC-MG, que fazem as engrenagens rodarem, muito obrigado!

Aos professores do passado e do presente, que não tenho como esquecer: Virgílio Almeida, Wagner Meira Jr. e Dorgival Olavo Guedes Neto. Vocês me despertaram a curiosidade e o prazer pela pesquisa. Sem esse passo inicial, nunca chegaria a este resultado. Obrigado!

Àqueles que esqueci, me desculpem. A cabeça é ruim. Mas meu muito obrigado também!

Obrigado também à CAPES e ao Departamento de Polícia Federal pelo apoio financeiro para este trabalho. Espero que outros possam se desenvolver a partir dele.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. Também contou com o suporte e apoio financeiro do Departamento de Polícia Federal.

"'North Korea? Really?'" ("'Coreia do Norte? Sério?'") – Geoff White na introdução do livro *The Lazarus Heist*. Este também era um comentário que eu comumente recebia ao dizer que pesquisava sobre *hackers* da Coreia do Norte. Eu compreendo você, Geoff.

RESUMO

A Coreia do Norte é um país peculiar por vários aspectos e está longe de ser uma potência econômica. Entretanto, possui um poder militar significativo e, mais que isso, detém a tecnologia de produção de armas de destruição em massa (ADM). Desenvolver e produzir esse tipo de armamento custa caro, e países com economias muito mais pujantes que a norte-coreana optaram por não o fazer. Outros começaram e desistiram, com a maioria optando por assinar acordos internacionais que limitassem a posse desse tipo de armamento. A Coreia do Norte permanece investindo este desenvolvimento (e nos seus militares), porque, sob o ponto de vista do país, e analisando sua história, essa escolha foi racional, de modo a conseguir demover os EUA de pretensas invasões, aumentar a influência regional e o prestígio global.

Há décadas, relatórios mostram que o financiamento destes projetos ocorre por meio de dinheiro obtido de formas ilícitas, como falsificação de dólares e cigarros, além de drogas de abuso e outras atividades criminalizadas em diversos países. Mais recentemente, acrescentou a este rol de atividades ações ofensivas cibernéticas. Esse trabalho assumiu como propósito analisar como a Coreia do Norte atua no espaço cibernético, no que tange a seus ataques cibernéticos. Para tanto, foi feita uma análise documental em materiais contemporâneos (livros, relatórios, notícias especializadas, dentre outros), de modo a identificar quais os objetivos de seus ataques e a que se destinam os recursos daí advindos, qual a participação do Estado em alianças com parceiros tradicionais ou outros atores do sistema internacional, quais parceiros ou atores são esses, que incentivos favorecem a manutenção de sua atuação no espaço cibernético, quais as principais ameaças a que está sujeita, quais as formas por que o país desenvolveu suas capacidades cibernéticas, quais são elas e como as utiliza.

Alguns dos usos atribuídos ao país são relatados e explicados, como o ataque de sabotagem à Sony Pictures Entertainment, em 2014, utilizado pela Coreia do Norte como uma forma de sinalização, furtos a bancos, como o Banco Central de Bangladesh, em 2016, e outras atividades cibernéticas pertinentes. Por fim, mostro como o uso de capacidades cibernéticas e a execução dessas ações com fins financeiros subverteram a posição do país, garantindo a ampliação de seu poder militar e, assim, mantendo sua relevância no sistema internacional, afetando a balança de poder.

Palavras-chave: Coreia do Norte, ameaças cibernéticas, capacidades cibernéticas, poder cibernético, balança de poder

ABSTRACT

North Korea is a unique country in many aspects, and it does not present itself as an economic power. However, it possesses significant military power and, beyond that, has the technology for production of weapons of mass destruction (WMD). Developing and producing this type of weaponry is expensive, and much more economically robust countries than North Korean have chosen not to do so. Others started and then gave up, with most opting to sign international agreements limiting the possession of this type of weaponry. North Korea continues to invest in this development (and in its military) because, from the country's perspective, and regarding its history, this choice was a rational one, aiming to deter the US from potential invasions and increase regional influence and global prestige.

For decades, reports have shown that the financing for these projects was made by money obtained through illicit means, such as counterfeiting dollar bills and cigarettes, as well as manufacturing illegal drugs and other activities that are criminalized in several countries. Recently, offensive cyber actions were added to this list of activities. This work has taken on the purpose of analyzing how North Korea behaves in cyberspace, regarding crimes. To meet this goal, I perform a documentary analysis of contemporary materials (books, reports, specialized news, among others), in order to identify the objectives of its attacks and the purpose of the resources derived from them, the participation of the state in alliances with traditional partners or other actors in the international system, which partners or actors are these, what incentives favor the maintenance of its criminal cyber activities, what are the main threats to the country, how they developed its cyber capabilities, which are them and how they are used.

Some uses attributed to the country of these capabilities are studied, such as the sabotage attack on Sony Pictures Entertainment in 2014, used by North Korea as a signaling action, bank heists, such as the Central Bank of Bangladesh in 2016, and other relevant cyber offenses. Finally, I show how applying these cyber capabilities and the financial result of them subverted the country's position, ensuring the expansion of its military power thus maintaining its relevance in the international system, affecting the balance of power.

Keywords: North Korea, cyberthreats, cybercapabilities, cyberpower, power balance

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAAI	*Association for the Advancement of Artificial Intelligence*
ADM	Armas de Destruição em Massa
AIEA	Agência Internacional de Energia Atômica
AIS	*Automatic Identification System*
ALN	Ação Libertadora Nacional
ANCiber	Agência Nacional de Cibersegurança
ANPD	Autoridade Nacional de Proteção de Dados
APCERT	*Asia Pacific Computer Emergency Response Team*
APT	*Advanced Persistent Threat*
ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
ATT&CK	*Adversarial Tactics, Techniques, and Common Knowledge*
BGP	*Border Gateway Protocol*
BID	Banco Interamericano de Desenvolvimento
BRICS	Brasil, Rússia, Índia, China, África do Sul
BWC	*Biological and Toxins Weapons Convention*
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CCHS	*Center for Cyber and Homeland Security*
ccTLD	country code *Top-level Domain*
CEPA	*Center for European Policy Analysis*
CERT	*Computer Emergency Response Team*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CFR	*Council on Foreign Relations*
CIA	*Central Intelligence Agency*
CISA	*Cybersecurity & Infrastructure Security Agency*
CNCiber	Comitê Nacional de Cibersegurança
COI	Comitê Olímpico Internacional
CPDOC	Centro de Pesquisa e Documentação de História Contemporânea
CRS	*Congressional Research Service*
CSIRT	*Computer Security Incident Response Team*
CSIS	*Center for Strategic & International Studies*
CWC	*Chemical Weapons Convention*
DARPA	*Defense Advanced Research Project Agency*
DDoS	*Distributed Denial of Service*
DIA	*Defense Intelligence Agency*
DNI	*Director of National Intelligence*
DNS	*Domain Name Service*
DoD	*Department of Defense*
DoJ	*Department of Justice*
DPRK	*Democratic People's Republic of Korea*, Coreia do Norte
EC3	*European Cybercrime Centre*
e-Ciber	Estratégia Nacional de Segurança Cibernética
EFF	*Electronic Frontier Foundation*
EIP	*The Economist Intelligence Unit*
ENISA	*European Union Agency for Cybersecurity* (até 2019 era *European Network and Information Security Agency*)
EO	*Executive Order*
ESI	Estudos de Segurança Internacional

ETDA	*Electronic Transactions Development Agency*
EUA	Estados Unidos da América
Europol	*European Union Agency for Law Enforcement Cooperation*
EIU	*Economist Intelligence Unit*
EIW	*Electronic Intelligence Warfare*
EW	*Electronic Warfare*
FBI	*Federal Bureau of Investigations*
FGV	Fundação Getúlio Vargas
FIRST	*Forum of Incident Response and Security Teams*
FMI	Fundo Monetário Internacional
FSB	*Federal'naya Sluzhba Bezopasnosti*, ou em russo, *ФСБ - Федеральная Служба Безопасности Российской Федерации*
GCI	*Global Cybersecurity Index*
GCHQ	*Government Communications Headquarters*
GDP	*Gross Domestic Product*
GGCiber	Gabinete de Gerenciamento de Cibercrises
GPS	*Global Positioning System*
GRU	*Glavnoye Razvedyvatel'noye Upravleniye*, ou em russo, *ГРУ -Гла́вное разве́дывательное управле́ние*
GSI	Gabinete de Segurança Institucional
HRW	*Human Rights Watch*
IA	Inteligência Artificial
IAEA	*International Atomic Energy Agency*
IANA	*Internet Assigned Numbers Authority*
IC3	*Internet Crime Complaint Center*
ICAN	*International Campaign to Abolish Nuclear Weapons*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICPO	*International Criminal Police Organization* (ou Interpol)
ICS	*Industrial Control System*
IETF	*Internet Engineering Task Force*
IGC	*Internet Governance Caucus*
IGF	*Internet Governance Forum*
IMO	*International Maritime Organization*
INMETRO	Instituto Nacional de Metrologia
Interpol	*International Criminal Police Organization* (ou ICPO)
IoT	*Internet of Things* (no português, Internet das Coisas)
IP	*Internet Protocol*
IPTF	*Infrastructure Protection Task Force*
IPv4	*Internet Protocol*, versão 4
IPv6	*Internet Protocol*, versão 6
ISI	*Information Science Institute*
ISO	*International Organization for Standardization*
IT	*Information Technology*
ITU	*International Telecommunications Union*
IXP	*Internet Exchange Points*
IWS	*Internet World Stats*
JTF-CND	*Joint Task Force-Computer Network Defense*
KCC	*Korea Computer Center*
KGB	*Komitet Gosudarstvennoy Bezopasnosti*, ou em russo, *КГБ Комитет Государственной Безопасности*
KHNP	*Korea Hydro and Nuclear Power Company*

KPTC	*Korea Posts and Telecommunications Co.*
KWP	*Korean Workers' Party*
LARC	Laboratório Nacional de Redes de Computadores
LBNL	*Lawrence Berkeley National Laboratory*
LGPD	Lei Geral de Proteção de Dados
MIT	*Massachusetts Institute of Technology*
MLA	*Mutual Legal Assistance*
MLAT	*Mutual Legal Assistance Treaty*
NATO	*North Atlantic Treaty Organization*
NCPI	*National Cyber Power Index*
NIS2	*Second Network and Information Systems Directive*
NIST	*National Institute of Standards and Technology*
NPT	*Nuclear Non-Proliferation Treaty*
NSA	*National Security Agency*
NSF	*National Science Foundation*
NSFNET	*National Science Foundation Network*
NSI	*Network Solutions, Inc*
NTIA	*National Telecommunications and Information Administration*
OEC	*Observatory for Economic Complexity*
OFAC	*Office of Foreign Assets Control*
OMPI	Organização Mundial da Propriedade Intelectual
ONG	Organização Não-Governamental
ONU	Organização das Nações Unidas
OPA	*Office of Public Affairs*
OPAQ	Organização para Proibição de Armas Químicas
OPCW	*Organization for the Prohibition of Chemical Weapons*
OS	Organização Social
OSI	*Open Systems Interconnection*
OSIC	Orientação de Segurança da Informação e Cibernética
OT	*Operational Technology*
OTA	*Office of Technology Assessment*
OTAN	Organização do Tratado do Atlântico Norte
PIB	Produto Interno Bruto
PIC	*Pyongyang Informatics Center*
PIIE	*Peterson Institute for International Economics*
PNCiber	Política Nacional de Cibersegurança
PNSI	Política Nacional de Segurança da Informação
PRK	*(Democratic) People's Republic of Korea*, Coreia do Norte
PTT	Pontos de Troca de Tráfego (de Internet)
RGB	*Reconnaissance General Bureau*
RI	Relações Internacionais
RIM	*Research In Motion*
RNP	Rede Nacional de Ensino e Pesquisa (antes de 1999 era Rede Nacional de Pesquisa)
ROK	*Republic of Korea*, Coreia do Sul
RUSI	*Royal United Services Institute for Defence and Security Studies*
SRBM	*Short-range Ballistic Missile*
SCADA	*Supervisory Control and Data Acquisition*
SIGINT	*Signals Intelligence*
SMTP	*Simple Mail Transfer Protocol*
SRI	*Stanford Research Institute*

SSIC	Secretaria de Segurança da Informação e Cibernética
SVR	*Sluzhba Vneshney Razvedki*, ou em russo, СВР - Служба Внешней Разведки
SWIFT	*Society for Worldwide Interbank Financial Telecommunication*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TED	Transferência Eletrônica Disponível
TFYQA	*Think for Yourself, Question Authority*
ThaiCERT	*Thailand Computer Emergency Response Team*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLD	*Top-level Domain*
TNP	Tratado de Não-Proliferação Nuclear
TTP	*tactics, techniques, and procedures*
UCLA	*University of California, Los Angeles*
UCSB	*University of California, Santa Barbara*
UE	União Europeia
UNODC	*United Nations Office on Drugs and Crime*
URSS	União das Repúblicas Socialistas Soviéticas
US	*United States*
USC	*University of Southern California*
USCYBERCOM	*United States Cyber Command*
VPR	Vanguarda Popular Revolucionária
WADA	*World Anti-Doping Agency*
WAN	*Wide Area Network*
WCI	*World Cybercrime Index*
Web	*World Wide Web*
WGIG	*Working Group on Internet Governance*
WMD	*Weapons of Mass Destruction*
WSIS	*World Summit on the Information Society*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A conexão de equipamentos à Internet e a necessidade de se estar e permanecer *online* já são realidade em várias sociedades, compreendendo 5,4 bilhões de usuários (67% da população mundial) em 2023, segundo relatório da União Internacional de Telecomunicações (ITU, do original em inglês *International Telecommunications Union*) (ITU, 2024, p. 1). Há um crescimento linear e constante de usuários de Internet no mundo, conforme o mesmo documento, segundo o qual 93% da população dos países de alta renda está conectada (também em 2023), ao passo que, em países menos desenvolvidos, somente 27% da população utilizava a internet no mesmo ano[1] (ITU, 2024, pp. 1-2). A ampliação contínua do número de usuários de Internet leva ao aumento da preocupação com a segurança, tanto dos equipamentos, quanto das transmissões dos dados. Se antes, por exemplo, os administradores de redes e sistemas se inquietavam com o sigilo das comunicações e a disponibilidade dos sistemas e do seu parque computacional, hoje é razoável que qualquer pessoa se preocupe com seus dados pessoais armazenados em um sítio de Internet, ou se uma transação bancária executada foi realizada, sem alteração, e para o destino correto.

Países também aderiram às tecnologias, promovendo diversos usos com distintas finalidades, como agilidade na comunicação governamental, oferecimento de serviços aos cidadãos e, claro, usos militares e na área de inteligência, como espionagem e sabotagem contra outros países. Por isso, devem se prevenir contra a má utilização dos sistemas e se proteger de outros Estados (SANGER, 2018; SEGAL, 2017; ROI, LYON, 2025, p. 67).

Nesse ambiente cada vez mais interligado, os dispositivos e redes computacionais oferecem oportunidades para também serem usados como ferramentas para a execução de crimes. Isso vale tanto para aqueles já definidos em normativos legais, como injúria, difamação e interceptação de comunicação, quanto para outros, que se sofisticaram, como furto, extorsão e sabotagem. Houve também o surgimento de novos crimes, como a invasão a sistemas computacionais e a exposição de dados pessoais. A expressão “crime cibernético” passou a ser usada para se referir a um conjunto desses crimes, cujo significado adotado neste estudo é aquele conferido pelo Glossário de Segurança da Informação[2], definido em portaria pelo Gabinete de Segurança Institucional (GSI) da Presidência da República do Brasil:

---

[1] O relatório considera países de alta renda aqueles assim classificados pelo Banco Mundial (disponível em: https://datahelpdesk.worldbank.org/knowledgebase/articles/906519), e países pouco desenvolvidos são os constantes na lista da ONU (disponível em: https://www.un.org/ohrlls/content/list-ldcs).

[2] O glossário navegável pode ser acessado em: https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1.

> **Crime cibernético**: ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores, utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar incidente, desastre cibernético ou obter lucro financeiro (BRASIL, 2021, n.p.).

Independentemente dos atores envolvidos, estes crimes apresentam custo alto e crescente para a sociedade. A Cybersecurity Magazine estima que este custo alcance US$ 10,5 trilhões em 2025, representando um incremento anual de 15% frente aos anteriores (MORGAN, 2024). A Statista projetou, no início de 2024, um custo de US$ 9,22 trilhões para aquele ano, com aumento incremental de aproximadamente 10% ao ano até 2028 (FLECK, 2024). Trata-se de duas metodologias distintas, mas ambos os cálculos alcançam valores acima do Produto Interno Bruto (PIB) de potências mundiais, como por exemplo o da Alemanha, aferido em US$ 4,59 trilhões pelo Fundo Monetário Internacional (FMI) (FMI, 2024a).

Importante destacar também que, em virtude da interconectividade da Internet, qualquer pessoa ou país pode ser alvo de ataques originados tanto dentro do seu território, quanto fora. E, independentemente da origem, o ataque pode ser executado por atores internos, externos ou uma combinação deles, já que praticamente as mesmas tecnologias computacionais e de conectividade estão disponíveis a ambos. Entretanto, cada país as utiliza de modos distintos, conforme os equipamentos usados pela população, a disponibilidade de conectividade, as capacidades técnicas e intenções de seu governo. Qualquer que seja o uso, o fato é que não há como fugir da conexão ao espaço cibernético e, por consequência, da exposição às ameaças que ele traz.

A Coreia do Norte, tema deste trabalho, não é exceção. Trata-se de um país conectado à Internet, exposto a seus riscos e que adotou usos bastante peculiares, além de deixar muitas pessoas curiosas. Afinal, é um país isolado em um mundo conectado, sobre o qual divulgam-se poucas notícias. Quando estas aparecem, normalmente envolvem assuntos assustadores, como desenvolvimento de mísseis balísticos e artefatos nucleares, ou balões contendo lixo e fezes enviados ao seu vizinho do Sul, em retaliação ao envio de dispositivos de memória de computador com músicas do estilo *k-pop* (CARVALHO, 2024). Aliás, a escolha por dispositivos de memória de computador contendo música e outras mídias é algo também curioso, considerando que a quantidade de norte-coreanos com acesso a computadores é bastante reduzida (IWS, 2024).

A capacidade da Coreia do Norte de desenvolver armas nucleares e mísseis balísticos tem origem após a separação da península depois da Segunda Guerra, nos anos 1950, como projeto de Kim Il-sung e apoio soviético. Na década de 1980 foi finalizado o primeiro reator

nuclear (em Yongbyon) e, em outubro de 2006, executado o primeiro teste nuclear (TERRY, 2021). Chama a atenção o fato de que o custo de desenvolvimento dessas armas é bastante alto, e sua economia não tem destaque. Segundo o *Observatory for Economic Complexity* (OEC) (SIMOES, HIDALGO, 2011), entre 220 países, a Coreia do Norte é o 182º em exportação e 219º em importações. O principal produto exportado, em 2022, foi o minério de tungstênio (US$ 30,9 milhões, correspondendo a 12,4% do total)[3]. A título de comparação, a Coreia do Sul, hoje, é um país desenvolvido e um dos maiores fornecedores de itens de alta complexidade e tecnologia, como circuitos integrados, o principal item de exportação em 2022 (totalizando US$ 121 bilhões, correspondente a 17,2% do volume de exportações)[4]. Comparando só os principais produtos exportados, trata-se de uma diferença significativa de quatro ordens de grandeza.

Nesse contexto, Perry Carpenter, executivo da área de segurança cibernética, e o jornalista investigativo Geoff White fizeram um comentário, de forma jocosa, no podcast *8th Layer Insights*, sugerindo que o principal produto de exportação da Coreia do Norte seria o "crime cibernético" (8th LAYER INSIGHTS, 2024, n.p.). Por mais que se tratasse apenas de um comentário informal, este se justifica: no relatório anual de ameaças da comunidade de inteligência do governo dos Estados Unidos da América (EUA), de 2024, consta que

> o programa cibernético da Coreia do Norte representará uma ameaça sofisticada e ativa de espionagem, **crime cibernético** e ataque. As forças cibernéticas de Pyongyang aperfeiçoaram e são plenamente capazes de alcançar uma variedade de objetivos estratégicos contra diversos alvos, incluindo um amplo conjunto de alvos nos Estados Unidos e na Coreia do Sul.
>
> A Coreia do Norte continuará a sua campanha cibernética, especialmente **furtos de criptomoedas; busca por abordagens variadas para lavar e sacar criptomoedas furtadas**; e manter um programa de trabalhadores de TI trabalhando no exterior para ganhar fundos suplementares[5] (EUA, 2024b, p. 22, tradução e grifo meus).

Quem acompanha notícias da área de segurança cibernética não estranha a relação entre estes crimes e a Coreia do Norte: há algum tempo sabe-se que o país é ativo, executando ações cibernéticas, principalmente por meio da Internet, como é demonstrado neste estudo. Tais

[3] Dados disponíveis em: https://oec.world/en/profile/country/prk.
[4] Dados disponíveis em: https://oec.world/en/profile/country/kor.
[5] Texto original: "North Korea's cyber program will pose a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea.
North Korea will continue its ongoing cyber campaign, particularly cryptocurrency heists; seek a wide variety of approaches to launder and cash out stolen cryptocurrency; and maintain a program of IT workers serving abroad to earn additional funds."

capacidades compõem o que Kim Jong-il chamou em 2013 de “espada de múltiplos propósitos” das Forças Armadas norte-coreanas para combater seus oponentes (KONG *et al.*, 2019, p. 1).

1.1 Definição do problema

Diante do que foi exposto, este trabalho trata da presença e atuação da Coreia do Norte no espaço cibernético. Isso envolve entender como, enquanto uma economia irrelevante em termos regionais e internacionais, inclusive submetida a sanções consideráveis (ONU, s.d.), exercer alguma influência política nos palcos internacionais. Neste último caso, é principalmente devido ao fato de possuir armas de destruição em massa (ADM). Mas o país também conseguiu desenvolver capacidades cibernéticas destacadas, sendo que parte delas é voltada à execução de ações como crimes financeiros, algo negativo aos olhos de diversos Estados e organismos internacionais, ainda mais que seriam ataques cibernéticos executados com o uso de sua estrutura governamental, inclusive contra alvos brasileiros (DENNESEN *et al.*, 2024).

A Coreia do Norte apresenta inovações técnicas ou tecnológicas nas suas capacidades cibernéticas, assim como outras potências da área, incluindo a execução de atividades como espionagem, sabotagem e subversão. A dimensão do país e sua economia limitada chamam a atenção por ter conseguido competir com as demais potências. Contudo, no seu caso, uma outra característica que o diferencia dos demais é o destacado objetivo de obter dinheiro cometendo o que comumente se chama de crimes cibernéticos (ou cibercrimes) (ONU, 2024a).

Simplificadamente, o problema de pesquisa que esta investigação busca responder é o seguinte:

Como a Coreia do Norte atua no espaço cibernético, no que tange a crimes?

1.2 Objetivos

Considerando a questão direcionadora, o estudo assume como propósito analisar o comportamento da Coreia do Norte no espaço cibernético, especificamente em atividades relacionadas a crimes cibernéticos. Para atingi-lo, esse objetivo geral se desdobra em outros específicos, expressos a seguir na forma de perguntas norteadoras para as quais passo a buscar respostas:

Considerando a presença da Coreia do Norte no espaço cibernético, quais são as principais ameaças a que ela está sujeita?

Como atacante, quais são seus objetivos quanto à execução desses crimes cibernéticos? A que se destinariam os recursos que o país obtém com eles?

Sabendo das peculiaridades norte-coreanas, como a grande quantidade de sanções a que o país é submetido e seu suposto acesso limitado a computadores e redes de comunicação, especificamente à Internet, de que forma a Coreia do Norte obteve e mantém suas capacidades cibernéticas?

Existe a participação ativa do Estado em alianças com parceiros tradicionais ou outros atores do Sistema Internacional, envolvendo o intercâmbio de técnicas e tecnologias relacionadas a essas capacidades? Quais seriam eles?

Por fim, que incentivos favorecem a manutenção de sua atuação criminosa no espaço cibernético?

1.3 Justificativa para o estudo

O impacto de incidentes cibernéticos, principalmente aqueles com fins maliciosos, são uma preocupação de todos os países. Um dos motivos é a dimensão do efeito econômico que podem alcançar. De acordo com o FMI, estes incidentes têm aumentado, duplicando desde o período pré-pandêmico da Covid-19. As estimativas da instituição são de perdas de pelo menos US$ 28 bilhões para a economia mundial, devido aos riscos cibernéticos, chegando inclusive a impactar na sua estabilidade (FMI, 2024b). Cabe esclarecer que a definição usada de "riscos cibernéticos", nesse caso, diz respeito à "combinação da probabilidade de ocorrência de incidentes cibernéticos e seu impacto"[6] (FINANCIAL STABILITY BOARD, 2018, n.p.). "Incidente cibernético", por sua vez, consiste em um evento ocorrido em um sistema de informação que comprometa sua segurança cibernética ou das informações nele processadas, armazenadas ou transmitidas, ou que viole suas políticas ou procedimentos de segurança ou, ainda, suas políticas de uso aceitável, sendo esse evento resultante de atividades maliciosas ou não (FINANCIAL [...], 2018).

O Internet Crime Complaint Center (IC3) estimou em US$ 12,5 bilhões as perdas potenciais devidas a crimes cibernéticos somente nos EUA. Esse centro pertence ao Federal Bureau of Investigation (FBI) e concentra as reclamações dos cidadãos e empresas daquele país, especificamente, quanto a crimes desse tipo (FBI, 2024a, p. 3). Ainda que os dois relatórios citados usem metodologias e foquem em públicos distintos, os valores chamam a atenção por estarem na ordem de grandeza dos bilhões de dólares.

[6] Texto original: "combination of the probability of cyber incidents occurring and their impact."

Muito já foi e continua sendo escrito sobre a península da Coreia, com sua população dividida em dois países numa guerra há mais de setenta anos, com um armistício assinado, sem um tratado de paz (SETH, 2020, p. 353; KIM, 2020). De acordo com relatório da The Economist Intelligence Unit (EIU), unidade de pesquisa do Economist Group, que calcula o índice de democracia dos países, a Coreia do Norte ocupa a posição de número 165 do índice (entre 167 países avaliados), sem liberdade civil (EIU, 2024, p. 13) e num regime classificado como autoritário (EIU, 2024, p. 47). Nem por isso o país se encontra completamente isolado no que tange ao uso de tecnologias recentes, como computadores e redes de comunicação: seus usuários representam 0,1% de sua população (RECORDED FUTURE, 2017; IWS, 2024).

Adicionalmente, trata-se de um país que incomoda: sabe-se que o comportamento do governo norte-coreano desagrada vários outros países. Isso pode ser visto pela quantidade de sanções que lhe são impostas pelo Conselho de Segurança das Nações Unidas desde 2006. Elas se referem ao bloqueio ou restrição de importações (por exemplo, de armamentos e artigos de luxo), exportações (como minerais, frutos do mar, petróleo e seus derivados), ao uso de embarcações, contratação de cidadãos norte-coreanos para trabalhar em outros países e transações financeiras (ONU, s.d.)[7].

Quanto ao Brasil, há ameaças domésticas com ataques bem particulares envolvendo características típicas do nosso país, como golpes bancários que incluem falsos boletos de cobrança. No espaço cibernético isso também ocorre, por exemplo, com falsos aplicativos bancários se apresentando como verdadeiros. Ainda, cidadãos brasileiros aplicam golpes similares em outros países, como a operação policial Grandorero, executada entre as polícias brasileira e espanhola, com apoio da Interpol, que prendeu brasileiros e espanhóis que aplicavam golpes na Espanha (SOUZA, BRAUN, 2024). Além dessas ameaças particulares, é claro que também estamos sujeitos àquelas que são comuns a países e empresas, envolvendo desde o furto de informações (espionagem) a crimes financeiros, como furto de criptoativos (DENNESEN *et al.*, 2024).

Estima-se que, entre abril de 2023 e março de 2024, 32% dos brasileiros foram vítimas de algum tipo de crime dessa natureza (CISO Advisor, 2024a). Um estudo recente da Mandiant, empresa estadunidense de segurança cibernética, especificamente sobre ameaças do tipo contra usuários e empresas brasileiros, identificou que diversos países, especialmente China, Coreia do Norte e Rússia, executam ações de espionagem contra o Brasil. Segundo esse estudo, a Coreia do Norte seria responsável por 31,7% dos desses ataques cibernéticos (DENNESEN *et*

[7] A lista de sanções enunciadas pelo Conselho de Segurança da ONU referentes à Coreia do Norte pode ser lido em: https://main.un.org/securitycouncil/en/sanctions/1718/materials.

al., 2024). Tal fato ainda é pouco estudado e reforça a necessidade de se compreender melhor qual a estrutura e a dinâmica norte-coreana nesse espaço.

1.4 Estratégia e método de pesquisa

Este trabalho é um estudo do caso da Coreia do Norte, considerando as atividades do Estado no espaço cibernético, utilizando a pesquisa documental para levantamento de dados.

O estudo de caso consiste numa metodologia usada no âmbito de várias ciências, incluindo as ciências sociais. Trata-se de uma estratégia de pesquisa que examina um fenômeno contemporâneo no seu contexto natural, utilizando distintas fontes de dados, sendo o número de variáveis maior que o de pontos de dados e o investigador não tem controle sobre o evento analisado (YIN, 2001, p. 32). Ressalta-se, também, que a pergunta que se pretende responder (*como*) relaciona-se mais à compreensão e explicação de um tópico específico do que propriamente à sua mensuração ou ao estabelecimento de relações causais. Nesse caso, portanto, a abordagem qualitativa se mostra a mais adequada.

Três casos foram escolhidos para serem estudados, na pesquisa, já que o compromisso com a profundidade limita a abrangência e o número de casos a serem investigados. O primeiro deles consiste em um ataque cibernético, atribuído ao governo da Coreia do Norte, a uma empresa japonesa, a Sony Pictures Entertainment, que teria como objetivo dissuadir a companhia de lançar um filme longa-metragem de comédia sobre o assassinato de um ditador, caricatura do líder norte-coreano (SANGER, 2018, pp. 124-151). Esse caso é apresentado na seção 5.2.1.

O segundo caso analisado é, na verdade, um conjunto de diversos ataques a bancos e corretoras, também atribuídos à Coreia do Norte, que resultaram no furto de ativos financeiros (inclusive criptoativos) (WHITE, 2022; WHITE, 2020, pp. 66-96). Esses ataques são discutidos no tópico 5.2.2.

Por fim, alguns outros casos que interessam ao objetivo do estudo são citados, na seção 5.2.3, a fim de mostrar a direção que as capacidades cibernéticas da Coreia do Norte têm tomado.

Foi feita uma análise holística desses casos, contemplando condições específicas que resultaram numa saída, aqui denominada crime cibernético, sendo o primeiro caso relacionado a espionagem, chantagem e vazamento de informações, o segundo a crimes financeiros, como furto e lavagem de dinheiro, e o terceiro a outros casos recentes e inovadores.

Destaca-se que o atual trabalho é *idiográfico*, ou seja, são tratadas características específicas e individuais do objeto estudado (atuação da Coreia do Norte no espaço cibernético)

que, por diversos fatores, dificilmente se desdobrariam numa regra geral a ser aplicada a outros países (o que seria o objetivo de um estudo *nomotético*)[8]. Aqui, portanto, não se busca gerar conhecimento generalizável, mas conhecer um caso atípico e extremo, que vale a pena entender, dentre outras coisas, pela sua singularidade.

A escolha de tratar desse universo traz consigo um risco, primeiro porque se refere a um caso delicado, na medida em que capacidades cibernéticas, ao contrário de grande parte do poderio militar, tendem a ser escondidas, não exibidas (BUCHANAN, 2020) – o que dificulta a coleta de dados. Segundo porque, envolvendo a Coreia do Norte, falo de um país notadamente reservado, sobre o qual é complexo obter informações detalhadas e confiáveis. Tudo isso trouxe, portanto, um desafio adicional que a pesquisa tentou ultrapassar recorrendo a distintas fontes de dados, sendo elas entendidas como documentos.

A pesquisa documental, conforme Sá-Silva *et al.* (2009, p. 5), consiste em "[...] um procedimento que se utiliza de métodos e técnicas para a apreensão, compreensão e análise de documentos dos mais variados tipos". Na mesma direção, Fonseca (2002) fala sobre a pesquisa documental da seguinte forma:

> A pesquisa documental trilha os mesmos caminhos da pesquisa bibliográfica, não sendo fácil por vezes distingui-las. A pesquisa bibliográfica utiliza fontes constituídas por material já elaborado, constituído basicamente por livros e artigos científicos localizados em bibliotecas. A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão etc. (FONSECA, 2002, p. 32).

Os dados que formam o *corpus* deste estudo, então, encontram-se em *documentos*, definidos pelo Dicionário Brasileiro de Terminologia Arquivística como sendo a "[u]nidade de registro de informações, qualquer que seja o suporte ou formato". (ARQUIVO NACIONAL, 2005, n.p.) Conforme o mesmo Dicionário, tais documentos são classificados em gêneros documentais, que são:

> [r]eunião de espécies documentais que se assemelham por seus caracteres essenciais, particularmente o suporte e o formato, e que exigem processamento técnico específico e, por vezes, mediação técnica para acesso, como documentos audiovisuais, documentos bibliográficos, documentos cartográficos, documentos eletrônicos, documentos filmográficos, documentos iconográficos, documentos micrográficos, documentos textuais. (ARQUIVO NACIONAL, 2005)

[8] Usando a terminologia de Gerring (2007), esse é um estudo de caso único (*single-outcome study*).

Interessante reparar no destaque dado por Oliveira quanto à seleção de fontes, segundo o qual é necessária uma análise cuidadosa das mesmas, visto que documentos não teriam passado por tratamento científico (OLIVEIRA, 2007 *apud* SÁ-SILVA *et al.*, 2009, p. 6). Nesse sentido, foi feita uma escolha criteriosa de quais seriam aqueles a serem considerados para embasar parte do estudo.

Em virtude, também, de o tema envolver algumas questões bastante técnicas, relatórios de empresas da área de informática e de segurança cibernética, como Mandiant, Microsoft, Recorded Future (empresa do Insikt Group) e Chainalysis, foram utilizados na construção desta tese. Especificamente na área de segurança cibernética, principalmente do que se chama de *Cyber Threat Intelligence*[9], as empresas têm especialização e uma estrutura maior, principalmente financeira, para analisar ameaças, do que órgãos de muitos governos, alguns dos motivos pelos quais se considera serem fontes confiáveis de dados.

Relatórios de organismos reconhecidos como o FMI, Banco Mundial e Organização das Nações Unidas (ONU) provêm informações importantes acerca da economia e capacidades estatais, tendo sido também consultados. Recorreu-se, igualmente, a organismos relacionados à Governança da Internet, como a ITU, sempre privilegiando informações de qualidade.

Para dados de capacidades relacionadas ao espaço cibernético, foram utilizados relatórios como os do *Belfer Center for Science and International Affairs* da Universidade de Harvard[10] e do *Council on Foreign Relations*[11] (CFR).

Como o tema "ataques cibernéticos" é contemporâneo e dinâmico, muitas das fontes sobre casos (recentes ou não) são reportagens jornalísticas investigativas, algumas com informações vazadas por funcionários de Estados, que não podem ser mencionadas. A especialização de parte dos jornalistas investigativos envolvidos tem gerado matérias com teor técnico e escrita inteligível para o público em geral. Alguns casos de maior repercussão ou importância, inclusive, tornaram-se livros. Por isso, também foram utilizados textos com conteúdo jornalístico para o estudo.

Por fim, alguns casos criminais envolveram polícias ou órgãos de inteligência de outros países e, portanto, seus relatórios ou indiciamentos foram consultados, como elaborados pelo FBI e a *Cybersecurity & Infrastructure Security Agency* (CISA), dos EUA.

[9] Numa tradução livre, Inteligência em Ameaças Cibernéticas.
[10] Sítio oficial: https://www.belfercenter.org/.
[11] Sítio oficial: https://www.cfr.org/.

1.5 Estruturação dos capítulos

Este trabalho estuda a Coreia do Norte e questões desse Estado com o espaço cibernético, especificamente quanto a ataques cibernéticos. Para desenvolvê-lo, foi construída a seguinte estrutura: o capítulo 1 consta desta introdução, em que se contextualiza o tema do estudo e se apresentam o problema de pesquisa, seus objetivos geral e específicos, a justificativa para a investigação e as opções metodológicas realizadas. O capítulo 2 contextualiza historicamente o espaço cibernético, conceitos relacionados à sua segurança e capacidades, mostrando algumas regulamentações existentes. O capítulo 3 traz questões e definições técnicas de ataques cibernéticos, sua atribuição e políticas de proteção. O capítulo 4 apresenta a Coreia do Norte, situando historicamente o país, suas capacidades em armas de destruição em massa, sanções impostas e sua relação com o Brasil. O capítulo 5, por sua vez, descreve a presença norte-coreana no espaço cibernético, suas capacidades cibernéticas e os usos ofensivos que faz delas. Nele, também é discutido se o Estado busca alianças para a troca de tecnologias relacionadas e como ele é alvo de ataques cibernéticos. Por fim, o capítulo 6 traz as considerações finais acerca do que foi apresentado, limitações e implicações práticas deste estudo, junto a contribuições e agenda de pesquisa proposta para o tema.

2 ESPAÇO, CAPACIDADES E REGULAMENTAÇÃO CIBERNÉTICOS

Nesta seção falo um pouco sobre conceitos da cibernética, como espaço cibernético e suas ameaças e capacidades, além de dar uma noção sobre regulamentos associados a este espaço, pertinentes ao estudo.

Às 22h30min do dia 29 de outubro de 1969, há pouco mais de 55 anos, era executada a primeira conexão (razoavelmente) bem-sucedida entre dois computadores na *Advanced Research Projects Agency Network* (ARPANET), nome da primeira rede de longa distância (em inglês *Wide Area Network*, WAN) que usou a tecnologia comutação de pacotes precursora da Internet. Esse momento foi chamado de "primeiro respiro da Internet" por Andrew Blum (2012, p. 48). O professor e pioneiro da Computação Leonard Kleinrock, da Universidade da Califórnia em Los Angeles (UCLA), supervisionava o estudante de programação Charley Kline enquanto enviava uma mensagem a outro computador remoto no *Stanford Research Institute* (SRI), localizado em Menlo Park, também na Califórnia. O professor observava o computador ao seu lado, conversando ao telefone com pesquisadores do SRI. Ele pediu ao seu aluno que digitasse 'l' e perguntou aos pesquisadores:

- "Vocês veem o 'l'?"

- "Sim, vemos o 'l'", responderam.

A seguir, o professor solicitou que o aluno digitasse a letra 'o':

- "Vocês veem o 'o'?"

- "Sim, vemos o 'o'."

Neste momento, o professor pediu que digitasse o "g" mas, em seguida, o computador do SRI deu pane e o comando não foi completado[12]. Esse caso explica por que se considera que a primeira transmissão pela Internet foi simplesmente 'lo', já que a família de protocolos em desenvolvimento para a ARPANET e usada naquele momento evoluiu, sendo adotada pela Internet até os dias atuais (WAZLAWICK, 2016, pp. 252-255; GROMOV, 1995; BLUM, 2012, p. 48). Como "família de protocolos", entendam-se os protocolos TCP/IP[13]. A ARPANET foi financiada principalmente pela *Advanced Research Projects Agency* (ARPA), hoje denominada *Defense Advanced Research Project Agency* (DARPA), do Departamento de Defesa (DoD, do original em inglês *Department of Defense*) dos EUA, e envolveu inicialmente poucos

[12] O intento era digitar a palavra 'login'.

[13] TCP/IP representa o acrônimo dos dois principais protocolos do conjunto: o *Transmission Control Protocol* e o *Internet Protocol*.

institutos[14]. Outros seguiram conectando-se à rede criada, ainda essencialmente acadêmica, até meados da década de 1990. Em 1980, o mesmo DoD padronizou sua rede interna, adotando oficialmente tais protocolos. Em janeiro de 1983, o TCP/IP também foi definido como o padrão oficial para a ARPANET sendo que, depois de alguns meses, nenhum computador se conectaria à Internet se não adotasse o protocolo IPv4 (*Internet Protocol*, versão 4)[15] (KLEINROCK, 2010). Importante destacar que o TCP/IP, ainda hoje, é o padrão utilizado na Internet, recebendo melhorias e atualizações como, por exemplo, o desenvolvimento do IPv6 (*Internet Protocol*, versão 6). A adoção deste mudou várias características em toda a rede, como por exemplo o endereçamento dos equipamentos e os protocolos de roteamento, com impactos em praticamente toda a malha de dispositivos e os sistemas a ela conectados. Outras informações técnicas sobre a família de protocolos TCP/IP estão disponíveis no APÊNDICE A.

No Brasil da década de 1970 houve a primeira intenção de se montar uma rede de computadores estadual unindo computadores das universidades do Rio Grande do Sul, e um primeiro ponto de conexão à ARPANET, o qual não seguiu em frente devido ao seu custo proibitivo. Outras iniciativas acadêmicas relacionadas foram desenvolvidas, como a criação do Laboratório Nacional de Redes de Computadores (LARC) em 1979. Tratava-se de uma entidade virtual, não de um espaço físico, que buscava integrar as iniciativas de pesquisas em redes de computadores, incluindo também a participação de empresas afeitas à atividade, como Telebrás e Embratel. Na década de 1980, o país contava com várias redes acadêmicas, sem a existência de padrão único de protocolos, nem interconexão entre elas. Entretanto, esta interconexão era o objetivo e, para isso, reuniões nacionais relacionadas ao tema foram feitas e houve diversas participações no exterior de pesquisadores em eventos de redes de computadores na mesma época. Um dos resultados foi que, em agosto de 1988, o anteprojeto de criação de uma rede nacional unificada foi apresentado pelo LARC, com o apoio de diversas entidades científicas, ao Ministério de Ciência e Tecnologia (SAVIO, 2006, pp. 74-78).

Em setembro de 1989, a Rede Nacional de Pesquisa (RNP)[16] era criada como um programa do então Ministério de Ciência e Tecnologia, com o objetivo de prover um

[14] Estes institutos começaram com o *Massachussets Institute of Technology* (MIT), a *University of California, Los Angeles* (UCLA) e o *Stanford Research Institute* (na época ligado à *Stanford University*), posteriormente conectando a *University of California, Santa Bárbara* (UCSB) e *University of Utah*. Em dezembro de 1969, equipamentos desses cinco institutos estavam interconectados à ARPANET.

[15] Principal protocolo do conjunto TCP/IP e responsável por, dentre outras funções, a de endereçar e rotear os pacotes entre os equipamentos da rede.

[16] Desde 1999 denominada Rede Nacional de Ensino e Pesquisa, e reconhecida desde 2002 não mais como o programa de um ministério, mas como uma Organização Social (OS).

backbone[17] acadêmico para a conexão das instituições de ensino e pesquisa, seguindo o formato de outras redes nacionais existentes em outros países. Sua primeira implantação foi completada em 1992 (RNP, 2019; SAVIO, 2006, pp. 89-90) e, apesar da orientação da Política Nacional de Informática vigente, que era de usar a família de protocolos *Open Systems Interconnection* (OSI), ela foi baseada em TCP/IP, a mesma arquitetura usada pela rede acadêmica dos EUA, a *National Science Foundation Network* (NSFNET)[18], desde a sua origem, em 1986 (SAVIO, 2006, pp. 79-100; GRIZENDI, STANTON, 2016, p. 209-212; DE CARVALHO, CUKIERMAN, 2015). Por consequência, assim que as conexões TCP/IP ficaram ativas, as redes acadêmicas conectadas ao *backbone* da RNP estavam efetivamente conectadas à Internet.

A expansão da Internet comercial em grande parte do mundo ocorreu na década de 1990. No Brasil não foi diferente: além do desenvolvimento da RNP e de outras redes menores em paralelo, em meados da década de 1990, houve um salto significativo na quantidade de provedores de acesso, de empresas com conexões dedicadas à rede, de empresas voltadas à comunicação *online* e prestação de serviços (SÁVIO, 2006, pp. 143-152).

Nesses mais de 50 anos tivemos o início da ARPANET, um projeto com financiamento originalmente militar que se transformou em algo acadêmico e, por fim, em uma rede comercial com funções e objetivos muito distintos do original. A presença de pessoas, empresas e governos aumentou exponencialmente com seu uso comercial, inclusive como plataforma para a prestação de serviços e o armazenamento e troca de arquivos e dados (BLUM, 2013). A presença na Internet de uma empresa ou organização na década de 1990, início da *World Wide Web* (WWW, ou simplesmente *Web*), normalmente envolvia a disponibilização de conteúdo institucional, como dados ou informações, sendo esta fase chamada de versão 1.0 da Web[19]. Posteriormente, houve a migração para seu uso como *plataforma*, como venda de itens, no caso de empresas, ou oferta de serviços a cidadãos, no caso de governos, o que se chamou de Web 2.0, o que possibilitou uma maior interação e troca de informações entre os atores envolvidos.

Como toda oportunidade vem acompanhada de riscos e ameaças, com o crescimento da Internet, a segurança cibernética (ou cibersegurança) relacionada a ela se transformou rapidamente em preocupação. Desde os anos 1970, militares envolvidos na prospecção de usos

[17] Termo normalmente utilizado para denominar uma infraestrutura principal de conexões de telecomunicações, cuja tradução seria "espinha dorsal".

[18] A NSFNET, patrocinada pela *National Science Foundation* (NSF), se originou a partir da ARPANET e objetivava a conexão de *campi* universitários para colaboração em pesquisas e compartilhamento de supercomputadores (SÁVIO, 2006, pp. 31-33).

[19] O'Reilly (2005) definiu os conceitos de Web 1.0 e Web 2.0 para diferenciar que a "nova" Web (a 2.0) apresentava um conjunto de princípios e práticas para ser aplicados em sítios da Internet, que não existiam na geração anterior. Cormode e Krishnamurti (2008) também mostram algumas das diferenças entre as duas gerações, incluindo alguns impactos analíticos e técnicos.

para as tecnologias computacionais que estavam sendo criadas percebiam que a segurança de tais sistemas seria algo mais holístico (WARNER, 2012). Com o acesso e o uso da Internet democratizados, ficou mais fácil perceber o mesmo: que essa segurança não envolve só o seu equipamento, mas algo multidisciplinar que inclusive abrange outros atores e fatores.

Se considerarmos que o conceito de segurança das Relações Internacionais, aplicável à sobrevivência de um país e de sua população, existe desde a formação do Estado e da sociedade, a segurança cibernética não seguiu o mesmo caminho. Na execução de projetos computacionais (tanto de equipamentos, quanto de sistemas), durante a história da computação, por muitas vezes, a segurança foi negligenciada em prol de diversas outras questões. Um marco significativo na mudança do pensamento da área ocorreu em 15 de janeiro de 2002, quando Bill Gates enviou um e-mail para todos os funcionários da Microsoft, uma empresa referência na área, informando sobre a nova iniciativa da empresa chamada de computação confiável (*trustworthy computing*) (GATES, 2002). Em outubro de 2002, um *white paper* elaborado continha os objetivos e meios para atingir o objetivo de se ter uma sistemas e equipamentos mais confiáveis e seguros. Como exemplo, a empresa passou a adotar, como padrão, princípios como *secure by design*, *secure by default* e *secure in deployment*, adotando a segurança como princípio desde o projeto, passando pela entrega e implementação de seus sistemas (MUNDIE *et al.*, 2002).

A participação dos Estados no espaço cibernético[20], do qual a Internet é um exemplo, e a definição desse espaço cibernético como um novo domínio militar trouxeram, também, consequências para os estudos de segurança internacional, bem como novas demandas e possibilidades de trabalho. A principal delas, talvez, seja conhecer esse novo domínio e garantir que sua população, dados e informações estejam seguros contra ameaças. Algumas destas, inclusive, já eram conhecidas e tão somente passaram a utilizar esse novo ambiente como, por exemplo, criminosos e espiões.

2.1 Cyber e Ciber

É comum que artigos e livros em inglês que tratam das questões de sistemas computacionais, sistemas de informação ou redes de computadores, iniciem conceituando o que seria algum termo somado ao prefixo *cyber* (*cyberspace, cybersecurity, cyberwar, cyberweapon, cyberthreat, cybercapabilities, cyberoperations, cyberdeterrence, cybercrime, cyberterrorism...*). Este estudo não é diferente. Segundo Thomas (2005, p. 7), em um certo

[20] Trato da definição desse conceito na seção 2.1.1.

dicionário haveria mais de 150 palavras utilizando este prefixo, algumas nem tanto relacionadas à c*yber age*[21] que nós vivemos.

A origem do termo (ou prefixo) *cyber* (ciber, em português) vem do grego arcaico *Κυβερνήτης*[22], que pode ser traduzido como "arte de navegar, pilotar" ou "timoneiro, leme, piloto", trazendo a ideia grega de independência dos navegantes que decidiam, de forma autônoma, o destino de suas navegações (LEARY, 1988, p. 256).

O termo foi escolhido, em 1947, por Wiener e Rosenblueth para nomear *cybernetics* (cibernética) a área interdisciplinar que, simplificadamente, estudaria "todo o campo da teoria de controle e comunicação, seja na máquina ou no animal"[23] (Wiener, 2019, p. 18, tradução minha). Isso envolveria toda interação com o mundo (por exemplo, entre o ambiente e indivíduos) e as consequências de tais interações ao serem retroalimentadas no mesmo sistema.

O primeiro uso mais conhecido do termo teria sido em 1960 por Manfred E. Clynes e Nathan S. Kline, quando cunharam a palavra *cyborg*, traduzido como ciborgue no português, que é a contração de duas palavras, *cybernetics* e *organism*, para representar um organismo humano conectado a sistemas de monitoramento e regulagem das suas funções físico-químicas (KIM, 2004, p. 208). Em 1972 a palavra deu título a um livro de Martin Caidin, *Cyborg*, que posteriormente virou uma quadrilogia. O ciborgue dessa obra, um piloto militar que sofreu um grave acidente, ao contrário da significação anterior, foi conectado a sistemas de monitoramento e regulagem citados, mas teve seu corpo reconstruído com peças biônicas que ampliavam as funcionalidades dos órgãos substituídos (KIM, 2004, pp. 208-209). O livro de Caidin inspirou a série de TV *The Six Million Dollar Man*, título traduzido como *O homem de 6 milhões de dólares*, que foi transmitido no Brasil pela TV Tupi e posteriormente pela Rede Bandeirantes (MUNERATTO, 2023).

No âmbito dos computadores, o prefixo teria sido usado pela primeira vez no neologismo *cyberspace*[24], pelo escritor canadense William Gibson na obra Neuromancer, de 1984, consistindo em

> [u]ma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz

[21] Termo utilizado pelo autor do levantamento, o qual pode ser traduzido como "ciber era" "ciber-era" ou "era cibernética".
[22] Pronúncia aproximada: *kybernetes*.
[23] Texto original: "entire field of control and communication theory, whether in the machine or in the animal".
[24] Significando "espaço cibernético", equivalente a "ciberespaço". O uso de palavras neste trabalho considera no português como ciber*termo* semelhante a *termo* cibernético.

> alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando (GIBSON, 2016, p. 77).

Em meados da década de 1990, o governo estadunidense formou um grupo de trabalho para emitir uma resposta ao relatório OTA-E-453 de junho de 1990, emitido pelo *Office of Technology Assessment* (OTA) do Congresso dos EUA, sobre a vulnerabilidade dos sistemas elétricos do país a ameaças físicas e sabotagens (EUA, 1990). Esse grupo de trabalho, então, enumerou tanto as ameaças indicadas pelo relatório, quanto outras, não relacionadas diretamente a aspectos físicos, mas com dependências do sistema elétrico, como por exemplo redes de telecomunicações, sistemas SCADA (do inglês *Supervisory Control and Data Acquisition*)[25], sensores e atuadores autônomos. Não havia um termo único que pudesse agrupar essas *outras* ameaças e muitos componentes do grupo de trabalho sequer conheciam os sistemas envolvidos em infraestruturas críticas das quais dependia seu funcionamento.

Relata-se que o advogado Michael Vadis, do Departamento de Justiça (DoJ), teria recém lido o livro *Neuromancer* e, numa conversa acerca de como chamar as *outras* ameaças, acabou por sugerir e defender no grupo o uso do termo *cyber* para descrevê-las. A questão, no entanto, é que o grupo não conseguiu, justamente, chegar a uma solução sobre como lidar com e mitigar essas ameaças, principalmente as *cyber*, já que envolviam uma miríade de questões e interesses (burocráticos, políticos, fiscais e corporativos). Em janeiro de 1996 o relatório foi entregue com essas questões, contendo em seu texto o termo *cyber*, pela primeira vez num documento oficial, agrupando as tais *outras* ameaças (KAPLAN, 2016, pp. 45-46). Em 15 de julho de 1996, o presidente dos EUA, Bill Clinton, emitiu a Ordem Executiva (EO, do original em inglês *Executive Order*) 13010 (“Proteção de infraestrutura crítica”) com o seguinte teor:

> Certas infraestruturas nacionais são tão vitais que sua incapacitação ou destruição teria um impacto debilitante na defesa ou segurança econômica dos Estados Unidos. Essas infraestruturas críticas incluem telecomunicações, sistemas de energia elétrica, armazenamento e transporte de gás e petróleo, bancos e finanças, transporte, sistemas de abastecimento de água, serviços de emergência (incluindo hospitais, polícia, bombeiros e resgate) e continuidade do governo. As ameaças a essas infraestruturas críticas se enquadram em duas categorias: ameaças físicas a bens tangíveis (“ameaças físicas”) e ameaças de ataques eletrônicos, de radiofrequência ou por computador aos componentes de informação ou comunicação que controlam as infraestruturas críticas (“ameaças cibernéticas”). Como muitas dessas infraestruturas críticas pertencem e são operadas pelo setor privado, é essencial que o governo e o setor privado trabalhem

[25] Sistemas SCADA consistem em uma tecnologia que permite a coleta de dados remotos e o envio de instruções. (BRANQUINHO *et al.*, 2014, cap. 1). São utilizados na automação, por exemplo, de plantas industriais, incluindo empresas de áreas de infraestrutura crítica, como sistemas de geração e distribuição de eletricidade, tratamento e fornecimento de água, telecomunicações, sistemas de transporte, dentre outros.

> juntos para desenvolver uma estratégia para protegê-las e garantir sua operação contínua.[26] (EUA, 1996, n.p., tradução minha).

A EO 13010 cria a Comissão Presidencial para a Proteção de Infraestrutura Crítica (*President's Commission on Critical Infrastructure Protection*) e, interinamente, a Força Tarefa de Proteção da Infraestrutura (IPTF, do original em inglês *Infrastructure Protection Task Force*) dentro do Departamento de Justiça, presidida pelo FBI. A força-tarefa visava "endereçar e prevenir crises que possam ter um impacto debilitante regional ou nacional"[27] (EUA, 1996, n.p., tradução minha). Posteriormente, em 1999, Clinton se mantinha bastante familiarizado e preocupado com o tema, tendo direcionado por anos parte do orçamento do país à proteção contra as ameaças cibernéticas (CLARKE, KNAKE, 2019).

Timothy Leary (1988, p. 263), em sua obra *The cyber-punk*, fala sobre a independência do indivíduo como "piloto de sua própria vida" e do *código cyberpunk TFYQA*[28]. A escolha do termo *cyber* nessa situação, pelo governo, e sua adoção por todos os organismos mais normatizados, rígidos e regulados do mundo (as polícias e Forças Armadas) pode, inclusive, ser vista com ironia.[29]

Retornando à Ordem Executiva, ela cita as ameaças cibernéticas (*cyber threats*) de um modo geral, agrupando nesse conceito "ameaças de ataques eletrônicos, de radiofrequência ou por computador aos componentes de informação ou comunicação que controlam as infraestruturas críticas" (EUA, 1996, n.p.). Atualmente, as ameaças são muito mais complexas do que as elencadas pelo documento, mas a sua edição trouxe à baila a discussão de como essas tecnologias influenciam a segurança de estruturas que tomamos como certas.

O *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), centro associado à Organização do Tratado do Atlântico Norte (OTAN), coordenou um estudo com especialistas para elaborar um manual não-vinculativo sobre a aplicação do direito internacional em operações cibernéticas (cuja versão atual é comumente chamada de *Tallinn manual 2.0* ou

---

[26] Texto original: "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ('physical threats'), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ('cyber threats'). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."

[27] Texto original: "better address, and prevent, crises that would have a debilitating regional or national impact".

[28] *Think for Yourself, Question Authority*, "pense por si mesmo, questione a autoridade", numa tradução livre.

[29] Timothy Leary morreu em 31 de maio de 1996, um mês e meio antes da emissão da Ordem Executiva citada.

somente *Tallinn manual*). Este documento define *cyber* como algo que "implica relação com a tecnologia da informação" (SCHMITT, 2017, p. 564).

No português (tanto europeu quanto brasileiro) convencionou-se utilizar o prefixo *ciber* associado a termos, da mesma forma como na língua inglesa, de modo a referenciar algo relacionado ao espaço cibernético.

A seguir trato de alguns conceitos que entendo como aplicáveis ao corrente estudo. Não o faço como conceituações únicas e definitivas, mas sim como as que mais se adequam para este trabalho, lembrando que elas podem variar conforme a área do conhecimento. Desse modo, pesquisadores das áreas de Telecomunicações, Computação, Direito ou Relações Internacionais podem ter diferentes interpretações, todas corretas e aplicáveis às suas respectivas realidades. Por fim, tecem-se considerações sobre o uso do termo por alguns países.

2.1.1 Espaço cibernético

Para Garvey (2021, p. 7), definir o espaço cibernético não seria um problema científico, mas um problema filosófico. Segundo ela, este seria "um espaço bidimensional que é paradoxalmente abstrato, concreto e evolui com o tempo"[30] (GARVEY, 2021, p. 7). As duas dimensões seriam corpo e mente, como um ser humano. E assim como nós, ambos interagiriam entre si, evoluiriam com o tempo e um não existiria sem o outro. Na visão da autora, o corpo compreenderia toda a infraestrutura, o mundo físico: equipamentos, conexões e dispositivos de armazenamento. A mente consistiria na organização do que flui através da infraestrutura, os conceitos, categorias, interpretações do que circula e do que está ali armazenado (GARVEY, 2021).

No início deste capítulo mostro um pouco da origem da Internet. Isso porque, na prática, é comum que as pessoas associem o espaço cibernético a esta rede mundial de computadores, sem identificar o que seria seu "corpo" e sua "mente". Como afirmou o filósofo Pierre Lévy, a Internet é "o símbolo e principal florão do ciberespaço" (LÉVY, 1999, p. 126). Contudo, o espaço cibernético vai além, incluindo outros tipos de rede de comunicação, tais como redes de telefonia, redes ponto-a-ponto e de transmissão por radiofrequência. Por isso, não é fácil defini-lo e, por vezes, a correlação com a Internet ou com redes de telefonia acaba se tornando mais simples para explicar algum conceito. O senador dos EUA pelo Alasca, Ted Stevens, numa audiência do Comitê para Comércio, Ciência e Transporte do Senado dos EUA, em 28 de junho

[30] Texto original: "a two-dimensional space that is paradoxically abstract, concrete, and evolves over time."

de 2006, afirmou que a Internet "não se trata de uma carreta, é uma sequência de tubos"[31] (STEVENS apud BLUM, 2013, p. 5). Não é preciso chegar a uma definição tão simplória. Num ambiente militar, ou mesmo onde o tráfego de dados é sensível seja pelo seu valor, seja porque são as redes de comunicação que mantêm a corporação funcionando, sua definição passa a ser bem mais importante. Kuehl, em 2009, fez um histórico de definições até aquela época, no âmbito dos conflitos cibernéticos e segurança nacional, e traçou a seguinte conceituação:

> O espaço cibernético é um domínio global no ambiente informacional, cujo caráter único e distinto é enquadrado pelo uso de eletrônicos e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações, por meio de redes interdependentes e interconectadas, usando tecnologias de comunicação de informação[32] (KUEHL, 2009, tradução minha).

Outros autores seguem a mesma preocupação em acrescentar que o espaço cibernético também abrange aspectos físicos e não físicos do espectro eletromagnético, assim como máquinas, interfaces, informações e pessoal especializado (FUTTER, 2018, pp. 22-23).

A definição mais ampla de Kuehl serviu de base para definições posteriores do Departamento de Defesa dos EUA (VAN PUYVELDE, BRANTLY, 2019). A atualmente utilizada pelo órgão, conforme suas publicações, indica que o espaço cibernético é

> [u]m domínio global dentro do ambiente informacional que consiste em redes interdependentes de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicação, sistemas computacionais e processadores embarcados e controladores[33] (EUA, 2021, p. 55, tradução minha).

As definições utilizadas pelo Estado brasileiro também seguem o mesmo caminho, como a constante no Glossário de Segurança da Informação da Presidência da República:

> "Espaço cibernético: espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente." (BRASIL, 2021, n.p.)

---

[31] Texto original: "It's not a big truck, it's a series of tubes (…)"

[32] Texto original: "cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

[33] Texto original: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

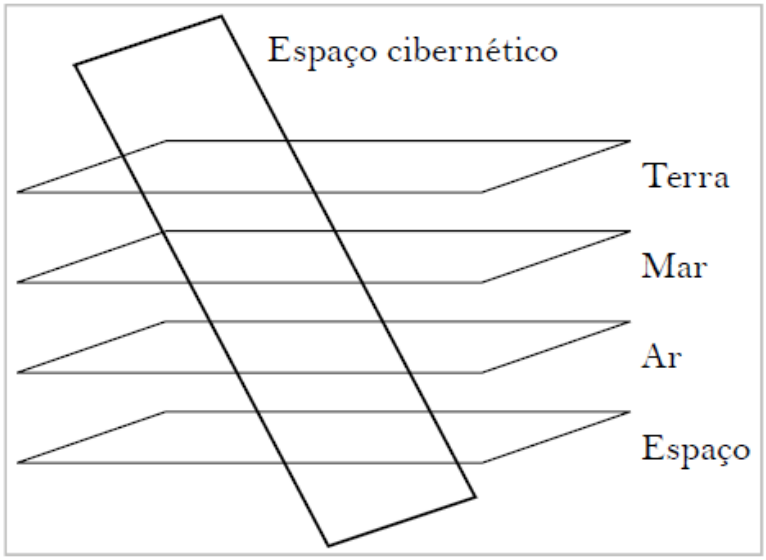
Nota-se que houve preocupação em deixar o conceito de forma abrangente. No que tange às Forças Armadas, o Ministério da Defesa definiu o mesmo conceito como "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas"[34] (BRASIL, 2016, n.p.). Neste caso, interessante constatar que se considerou, inclusive, o fato de haver dispositivos computacionais que não estejam conectados em rede.

Chamo a atenção para o fato de que as definições apresentadas desconsideraram um ponto que acredito ser importante na definição de Kuehl: ambas não tratam especificamente do espectro eletromagnético. Consideram pertinentes somente as redes que eventualmente o utilizem. Da mesma forma, Kuehl fala sobre redes interconectadas, deixando claro que a Internet não é equivalente ao espaço cibernético, mas que faz parte deste, assim como quaisquer outras redes de comunicação. Entretanto, é notório que muitas das redes de comunicação convergiram para a Internet, o que inclusive justifica a confusão e uso intercambiável entre os dois conceitos.

Importante destacar que o espaço cibernético não se trata exatamente de um domínio físico, mas virtual, criado pelo homem para seu uso, que se utiliza (e depende) dos demais domínios físicos (terra, mar, ar e espaço). A Figura 1 ilustra, de forma simples, como podemos perceber estes domínios e como esse "quinto domínio" (como também é identificado) perpassa todos os demais.

[34] Apesar de não estar explícito, como há o uso do termo "ciberespaço" no mesmo documento, acredito que os dois termos sejam tratados como sinônimos.

Figura 1 – Presença transversal do espaço cibernético



Fonte: Ventre (2012a, tradução minha).

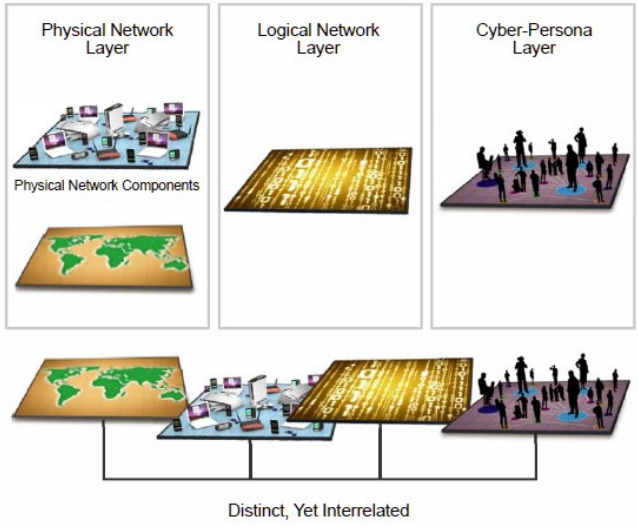
Considerando os "cinco domínios" e o fato de o espaço cibernético ter sido construído pelo homem, Clarke e Knake chamam a atenção de que "é um atributo positivo do espaço cibernético que, uma vez que uma arma [cibernética] tenha sido usada e descoberta, ela pode ser bloqueada. Isso é o equivalente a mudar a atmosfera para que bombas não mais caiam"[35] (CLARKE, KNAKE, 2019, p. 6, tradução minha). Outro corolário que se pode tirar do fato de que o espaço cibernético é um produto humano é que cada país pode estruturá-lo e alterá-lo independentemente dos demais. Entretanto, tal estruturação e alteração não são tão simples. Como ilustração, tem-se uma rede como a Internet, que utiliza um conjunto padrão de protocolos (TCP/IP) com uma única forma de endereçamento e roteamento (os endereços IP) para todos os equipamentos, o que os faz os compatíveis e comunicáveis. Ou seja, se algum país não utilizar esse padrão, ele não se conectará à Internet. Por outro lado, o simples uso do mesmo conjunto de protocolos não inclui qualquer rede na Internet, mas a deixa *apta* para se conectar à mesma, satisfeitas outras condições como: conexão a uma outra rede, registro em servidores mundiais de *Domain Name Service* (DNS, Sistema de Nomes de Domínios, numa tradução livre[36]) e designação de uma faixa ou sequência de endereços IP para seu uso.

Em alguns casos, pode ser útil abstrair certos componentes e atores dentro do espaço cibernético. Alguns pesquisadores e organismos fazem-no utilizando de três a sete camadas. Por exemplo, o DoD divide o espaço em três camadas, enquanto o Ministério da Defesa do

[35] Texto original: "It is a positive attribute of cyberspace that once a weapon has been used and discovered it can be blocked. That is the equivalent of changing the atmosphere so that bombs can no longer fall."
[36] A Seção 2.2.1 à frente explica sobre esse conceito.

Reino Unido o divide em sete. Independentemente do modelo utilizado, é importante destacar que as camadas são inter-relacionadas e não "funcionam" sozinhas. Para o trabalho aqui proposto, o modelo do DoD parece adequado, o qual separa o espaço cibernético nas seguintes três camadas: rede física, rede lógica e *cyber-persona*, as quais são ilustradas na Figura 2 a seguir.

Figura 2 – Modelo de camadas do espaço cibernético, conforme o DoD



Fonte: EUA (2018, p. I-3).

A camada de rede física se refere à infraestrutura e aos dispositivos físicos que proveem armazenamento, transporte e processamento da informação dentro do espaço cibernético. A camada de rede lógica, por sua vez, trata da relação entre os dispositivos da rede de forma a se abstrair da rede física, baseado na lógica de programação. Um dispositivo existente na rede lógica pode significar vários componentes físicos, e uma conexão lógica entre dois pontos indica que há comunicação viável entre eles, feita possivelmente a partir de várias conexões físicas. Por fim, a camada *cyber-persona* indica um ator ou entidade que se utiliza das redes lógicas e físicas. Esse ator pode ser um usuário real, um autômato que executa tarefas programadas (normalmente chamados de *bots*) ou uma conta compartilhada entre usuários dentro de um sistema (EUA, 2018b; VAN PUYVELDE, BRANTLY, 2019). Ameaças a esse domínio são percebidas e protegidas de formas diferentes, conforme o alvo.

A identificação de uma camada envolvendo pessoas se torna mais interessante, alterando a percepção, natureza e escopo dos ataques. Futter (2018, p. 23), inclusive, separa o que ele chama de "desafio cibernético" (*cyber challenge*) em quatro camadas[37] para análise:

[37] No livro ele usa a expressão domínio de análise ("*domains of analysis*"), mas aqui uso *camadas* para manter coerência com os modelos exemplificados e não confundir com os domínios anteriormente citados.

físico/mecânico, lógico, informacional e humano/cognitivo. Isso porque se pode, por exemplo, caracterizar como ameaças a usuários de sistemas como ameaças ao espaço cibernético, seja para obtenção de suas identidades, ou utilizá-los como vetor de algum ataque.

Retornando às definições, o *Tallinn manual* do CCDCOE define o espaço cibernético como um "ambiente formado por componentes físicos e não-físicos para armazenar, modificar e trocar dados por meio de redes de computadores"[38] (SCHMITT, 2014, p. 564).

Com relação à Internet, há aproximadamente três décadas, houve uma crença de que se tratava de uma "terra sem lei", "terra de ninguém", e que "na Internet ninguém sabe que você é um cachorro", parafraseando o famoso cartum de Peter Steiner, publicado em 1993 no *New York Times*[39], com o anonimato sendo a regra para todos os usuários. Por algum tempo, inclusive, usou-se o termo *netizen* (cidadão da rede, numa tradução livre), sugerindo que os Estados teriam pouca ou nenhuma gerência sobre o que ali circularia. O professor do MIT Nicholas Negroponte mostrou como era a visão da época, argumentando quão difícil seria a regulamentação do tráfego da Internet e do seu acesso por cidadãos locais. Ele chegou a afirmar que seria praticamente impossível tal tarefa, e que, se isso ocorresse, tolheria a criatividade dos seus usuários (NEGROPONTE, 1995).

Um dito famoso na *Internet Engineering Task Force* (IETF) é o aforismo de 1992, pronunciado por Dave Clark, um dos pioneiros da Internet, sobre como as decisões são tomadas por eles: "Nós rejeitamos: reis, presidentes e eleições. Nós acreditamos em: consenso aproximado e código executável"[40] (CLARK, 1992, n.p., tradução minha). A IETF consiste numa organização composta de pessoal técnico especializado em redes (engenheiros, projetistas, operadores, fornecedores) que se concentra, principalmente, em criar padrões de transporte, roteamento, segurança e afins, relativos à Internet, e emitir os documentos com suas especificações (DeNARDIS, 2014; CHOUCRI, 2012; CARPENTER *et al.*, 2000).

Essas passagens evidenciam duas características da Internet da época. A primeira mostra a questão do anonimato e da inexistência de controles de fronteira, diante da ausência da necessidade de o usuário ser identificado ao acessar um sítio, uma página ou um arquivo qualquer, em um computador que se encontra fisicamente fora das fronteiras de seu país de

---

[38] Texto original: "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."

[39] O cartum pode ser visualizado em https://images.squarespace-cdn.com/content/v1/5c3e06ceb98a78156ebe8c8c/1549921000369-QQZ5T9343P07T69VMS36/1993+07+05+internet+high+res.HG+On+t.jpg?format=1000w. Acesso em: jun. 2024.

[40] Texto original: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code." O conceito de *rough consensus* é algo muito caro à IETF para sua tomada de decisões. Ele é explicado na página "*The Tao of IETF*" acessível em: https://www.ietf.org/participate/tao/.

residência (ou por onde esteja de passagem). Não há postos de controle de passaportes onde o usuário (*netizen*) se identifique, bem como não há exigências de obediência a legislações dos mesmos países de origem ou de trânsito dos dados antes da chegada ao destino.

A segunda passagem, por sua vez, ilustra que as decisões anteriormente tomadas quanto à arquitetura da rede e seus sistemas, supõe-se, eram pragmáticas e definidas por pessoal técnico capacitado no assunto. Pode parecer estranho, mas não eram levados em conta certos valores caros ao mundo atual, como a democracia, nem consultas públicas. O consenso entre os pares (técnicos) já seria suficiente.

Com o passar dos anos, muito do que se acreditava sobre o futuro da rede se provou errado, inclusive as características anteriormente descritas. A Internet acabou sendo tomada por choques de realidade quando passou a servir, por exemplo, como um local de comércio, sendo que as regras aplicadas às empresas *brick-and-mortar*[41] tiveram que ser também aplicadas àquelas no ambiente *online*. Algumas modalidades de crimes já existentes passaram a ser executadas via Internet, enquanto novos crimes foram tipificados. Apareceram, portanto, questões inéditas sobre qual a competência para a sua investigação, quais os meios de produção de provas e, claro, a possibilidade de novas tipificações legais mais específicas.

Por fim, o espaço cibernético se tornou um palco de competição estratégica entre as grandes potências, com outros países participando dele de forma estratégica com o desenvolvimento de suas capacidades cibernéticas. Domingo (2025, pp. 266-268) cita cinco países como atores dentro da competição estratégica nesse ambiente: Rússia, China, EUA, Irã e Coreia do Norte. Mas não são os únicos: Israel, Itália, Índia, Reino Unido, Austrália, Países Baixos, Dinamarca, Suécia, Grécia e França são outros exemplos (UREN, 2024; JACOBSEN, 2017).

2.1.2 Segurança e defesa cibernéticas

Não é incomum que os conceitos de segurança e defesa cibernética sejam utilizados como sinônimos e, por vezes, a diferença de aplicação de ambos é sutil. Com relação ao Brasil, o Glossário de Segurança da Informação ainda diferencia dois conceitos: segurança cibernética e segurança da informação. Ambos são apresentados no Quadro 1, a seguir, para facilitar a comparação de seus textos.

[41] Essa expressão, que traduzida literalmente significa 'tijolo-e-argamassa', é usada em ambientes organizacionais para representar empresas cujo negócio envolve a necessidade de uma instalação física como um escritório, loja ou fábrica. A este tipo de empresa, negócios *online* na Internet serviriam como contraponto.

Quadro 1 – Definições conforme Glossário de Segurança da Informação

Termo	Definição
Segurança cibernética	"Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis."
Segurança da informação	Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações."

Fonte: Brasil (2021, n.p.)

Percebe-se que, apesar de haver certa relação entre os dois, o primeiro conceito é mais amplo, pois que aplicado à operação e disponibilidade de sistemas, e o segundo se aplica mais às informações neles armazenadas. Com relação às Forças Armadas, o seu glossário dá a seguinte definição para segurança cibernética: "arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2016, n.p.).

Já o termo "defesa cibernética" normalmente abrange a proteção de sistemas no espaço cibernético que, em geral, envolvam a segurança nacional e questões como soberania. A definição constante no Glossário de Segurança da Informação da Presidência da República define a defesa cibernética como

> [a]ções realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente. (BRASIL, 2021, n.p.)

A definição das Forças Armadas, em seu glossário, vai na mesma direção:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (BRASIL, 2016, n.p.)

Ambas as definições trazem uma visão de que o espaço cibernético é um palco de ações ofensivas como aquelas de obtenção de dados de inteligência (neste caso seria uma fonte cibernética[42]), ou mesmo a execução de ações que atinjam opositores, desde que estas

[42] A fonte cibernética é considerada complementar a outros tipos de fontes, como por exemplo humana, sinais e imagens (BRASIL, 2016, p. 119).

apresentem interesse para a preservação da defesa nacional (como, por exemplo, preservação de território, soberania e outros).

Dunn Cavelty desenvolveu vários estudos sobre a securitização da segurança cibernética, utilizando vários tipos de documentos relacionados ao tema, vindos de diversos países. Num estudo de 2013, ela mostra que a interpretação do conceito dada por uma certa comunidade de atores variava, principalmente, de acordo com o objeto referência que deve ser mantido seguro. Com isso, cada uma dessas comunidades percebe um grupo distinto de ameaças como sendo o principal. Sob esse prisma, ela dividiu o campo da segurança cibernética em quatro agrupamentos (*clusters*), cada um com um grupo de atores com características próximas, ou seja, com o mesmo tipo de objeto a ser protegido e um conjunto similar de ameaças a ser repelido. Esse resumo encontra-se traduzido no Quadro 2 a seguir.

Quadro 2 – Mapeamento do campo da segurança cibernética

	I	**II**	**III**	**IV**
Ator principal	Subcultura *hacker* Especialistas em segurança computacional	Atores de negócios Empresas de antivírus Forças da lei Comunidade de Inteligência	Órgãos de defesa civil / Segurança nacional	Militares
Objeto de referência	Computadores Redes computacionais	Setor privado (redes corporativas) Informações confidenciais (redes governamentais)	Informações de infraestruturas críticas Sociedade (particularmente seu "funcionamento")	Redes de Forças Armadas (redes militares) Informações sobre infraestruturas críticas
Ameaças	*Malware* Ataques a redes Hackers (todos os tipos)	Ameaças Persistentes Avançadas (APT[43], *malware*[44]) Criminosos cibernéticos (não-estatais) Espionagem cibernética (estatal)	Interrupção de infraestruturas críticas Efeitos cascata Terroristas cibernéticos (não-estatais) Comandos cibernéticos (estatais)	Ataques (catastróficos) a infraestruturas críticas Terroristas cibernéticos (não-estatais) Espionagem cibernética (estatal) Comandos cibernéticos (estatais)

Fonte: Dunn Cavelty (2013, p. 109, tradução minha).

Interpretando o agrupamento identificado como I no quadro anterior, ele identifica que, para os atores da área técnica, o principal objeto a ser segurado são os computadores e suas redes, sendo estes o que a autora chamou de objetos de referência. Estes atores, portanto, perceberiam como principais ameaças aquelas que atingissem tais equipamentos ou estruturas, determinando um ataque de *malware*, por exemplo, como relevante. Por sua vez, órgãos de

[43] A definição de Ameaças Persistentes Avançadas (APT, do original em inglês *Advanced Persistent Threats*) é apresentada mais à frente no texto.
[44] Uma explicação do que é *malware* é apresentada à frente no texto.

segurança nacional se preocupariam mais, por exemplo, com o funcionamento da sociedade e, por isso, focam o funcionamento das infraestruturas críticas. Outra forma de perceber isso é utilizando o modelo em camadas do DoD apresentado na seção anterior, como se tratássemos da mesma forma, na camada física, um usuário doméstico de Internet ou um órgão governamental. Há diferenças não só técnicas, mas também de impacto caso haja interrupção da conexão de uma residência ou do citado órgão.

Como já relatado, a rede com tecnologia de comutação de pacotes originária da Internet, ARPANET, era um projeto militar, depois sendo transformada em uma rede acadêmica e, em seguida, tendo um viés comercial. Isso não significa que os militares tenham saído da rede, mas que segmentaram suas redes, utilizando a mesma tecnologia TCP/IP, e, posteriormente, também as conectaram à Internet. Hoje, também, temos a presença de órgãos governamentais e a prestação de serviços, vendas ou compartilhamento de informações por meio da Internet. É por questões como esta que se discute, dentro da teoria da securitização, sobre o fato de o espaço cibernético ser ou não securitizado. A mesma Dunn Cavelty estudou o assunto e mostra que, conforme o ator que observa a rede, ele apresentará preocupações que justifiquem a securitização ou, pelo menos, que se trata de um ativo que precisa ser protegido por ser base importante para sociedades atuais (DUNN CAVELTY, 2008; DUNN CAVELTY, 2020). É por isso que entendo não ser estranho haver tantas definições distintas para os mesmos vocábulos: trata-se de algo inerente ao tema estudado, conforme a visão que se tem do assunto: seja civil ou militar, técnica ou não, governamental ou não.

Buzan e Hansen (2012) questionam uma suposta desconsideração dada ao assunto de "segurança em informática". Segundo os autores,

> [s]egurança em informática é um termo técnico utilizado por cientistas da computação para referir-se a problemas ligados aos programas e equipamentos de informática, alguns deles *bugs* acidentais, outros, resultado de ataques externos de pessoas maldosas. A resposta padrão dos ESI [Estudos de Segurança Internacional] é que esses conceitos carecem do drama e da urgência da segurança "nacional/internacional", que lidam com (...) ameaças "técnicas", e não político/militares, no caso da segurança em informática. Apesar de uma similitude semântica com segurança (nacional), não há semelhança substancial e discursiva (BUZAN, HANSEN, 2012, p. 43).

Nos meios mais técnicos o conceito de "segurança de informática" é limitado e se aplica, normalmente, a sistemas computacionais e conexões de rede. Entretanto, dentro das Relações Internacionais entende-se que sua importância varia conforme o assunto ao qual se relaciona, ou o ator afetado pela ameaça impedida ou mitigada por algum sistema de segurança cibernética. Assim, acredito que os autores considerem que o alcance da sua definição seria

mais amplo, não restrito e, portanto, estariam usando tal expressão como sinônimo para segurança cibernética.

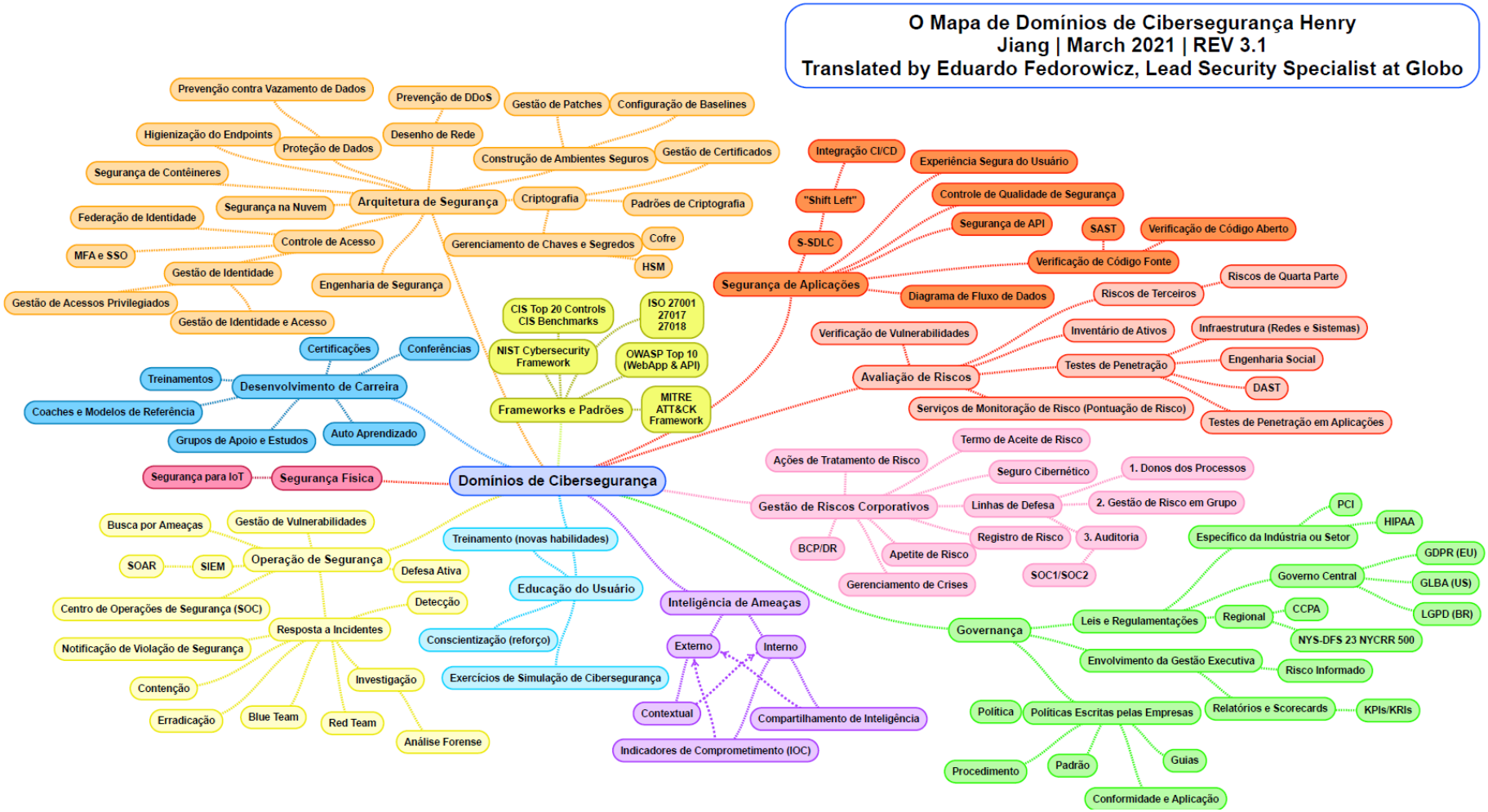
Noutra visão dentro das Relações Internacionais, Choucri (2012, pp. 40-39) argumenta que a segurança nacional atualmente envolve quatro dimensões interconectadas: segurança externa, segurança interna, segurança ambiental e segurança cibernética. A primeira diz respeito à defesa do território contra ameaças externas, algo central dentro das teorias realistas de Relações Internacionais. A segunda é referente às instituições de governança e o combate às ameaças que atingem a estabilidade interna do Estado. Em seguida, a questão da segurança ambiental envolve a capacidade do Estado de prover as demandas da população, de acordo com os recursos naturais existentes e a tecnologia disponível para utilizá-los. Por fim, para a autora, a segurança cibernética "refere-se à capacidade de um Estado de se proteger, e a suas instituições, contra ameaças, espionagens, sabotagem, crime e fraude, identificar ameaças e outras interações e transações eletrônicas destrutivas"[45] (CHOUCRI, 2012, p. 39, tradução minha).

Para se ter uma visão mais ampla, voltada principalmente para contextos técnicos e administrativos corporativos, Jiang (2021) montou um mapa mental com os diversos domínios da grande área de segurança cibernética[46], ilustrado a seguir na Figura 3. Nota-se a grande quantidade de áreas em que a segurança cibernética se divide, relacionando-se inclusive a outros campos do conhecimento, como as ciências sociais aplicadas, por exemplo, no que tange à governança. Em seguida cito alguns exemplos práticos desses domínios.

[45] Texto original: "It refers to a state's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identify theft, and other destructive e-interactions, and e-transactions."

[46] O autor usa o termo *cybersecurity* no original em inglês e, em português, o tradutor usou o termo cibersegurança que, como já afirmado anteriormente, considera-se equivalente ao usado no decorrer deste texto.

Figura 3 – O Mapa de Domínios da Cibersegurança, por Henry Jiang, versão 3.1



Fonte: Jiang (2021, traduzido por Eduardo Fedorowicz).

Quando se trata de arquiteturas de segurança, consideram-se, claro, questões técnicas como qual a estrutura da rede, seja ela física, considerando o tipo de conexão física (cabeamento estruturado, fibras ópticas, equipamentos de rede), ou lógica, que abarca a configuração envolvendo separação de endereços IP, filtros de segurança e restrições de acesso diversas. Isso está relacionado a outras questões técnicas referentes a controles de acesso, aplicáveis conforme a estrutura da organização. Por exemplo, todos os dados e relatórios do setor de comunicações de um ministério não precisam estar disponíveis para o departamento de cerimonial, ou para o de planejamento estratégico. Apesar da hierarquia, talvez nem seja conveniente o ministro ter acesso irrestrito a tais dados e relatórios, mas somente a uma parte deles. Essas questões podem envolver a configuração de equipamentos, mas também de políticas internas de cada órgão da administração pública ou empresas. A gestão de acesso também é importante nos casos de violação da segurança de uma rede ou das credenciais de acesso ao sistema de um usuário[47]. Caso haja tal violação, se ela não for descoberta a tempo houver utilização indevida, quem o acessar terá o mesmo tipo de acesso que o usuário tinha e, sendo este limitado, restringe os arquivos a serem furtados, alterados ou removidos.

O uso de arcabouços (*frameworks*) e padrões internacionais pode permitir a uma empresa, por exemplo, obter certificações que permitam sua conexão a redes e sistemas de terceiros, além de facilitar a implantação de novos equipamentos na rede e estruturar novos sistemas. Trabalhar sem se atentar a padrões internacionais pode também aumentar o tempo de resposta a um incidente, dificultando a sua identificação. Uma vez identificada uma violação de segurança, arcabouços como o MITRE ATT&CK permitem classificá-la, facilitando, dentre outras ações, a execução de contramedidas e posterior auditoria.

Como último exemplo, cito o fato de a segurança física também estar relacionada à segurança cibernética. Permitir que algum indivíduo externo tenha acesso físico a cabos, equipamentos de rede ou mesmo a dispositivos computacionais são falhas sérias que, se não houver algum tipo de monitoramento, podem permitir, por exemplo, que dados sigilosos sejam interceptados (ou mesmo alterados), equipamentos sejam desligados, redes de transmissão sejam interrompidas, ou até programas ou hardwares, com os mais diversos objetivos, sejam instalados à revelia do órgão ou empresa.

Muito após as redes e sistemas de informação do Pentágono serem avaliados e declarados como inseguros ou com falhas com o exercício *Elegible Receiver 95* (ER95), em 1998 foi criada a *Joint Task Force – Computer Network Defense* (JTF-CND, numa tradução

[47] Um exemplo simples de violação de segurança de credenciais de acesso seria o vazamento do usuário e senha de um servidor do órgão.

livre, Força Tarefa Conjunta – Defesa de Redes Computacionais) para supervisionar e cuidar da segurança cibernética das redes do DoD. Após várias configurações, dez anos depois, em 23 de julho de 2009, era criado o *United States Cyber Command* (USCYBERCOM), com a seguinte missão:

> O USCYBERCOM planeja, coordena, integra, sincroniza e conduz atividades que: direcionam as operações e defendem redes específicas do Departamento de Defesa; e prepara para que, quando comandada, conduza operações do espaço cibernético de amplo espectro para habilitar ações em todos os domínios, garantir a liberdade de ação aos EUA e aliados, e negar o mesmo aos nossos adversários[48] (EUA, s.d.a., tradução minha).

Sua missão atual é "direcionar, sincronizar e coordenar o planejamento e as operações do espaço cibernético – para defender e promover os interesses nacionais – em colaboração com parceiros nacionais e internacionais"[49] (EUA, s.d.b., n.p., tradução minha). Ou seja, trata-se de um comando específico para tratar, inclusive, de operações cibernéticas ofensivas, não só monitorar e defender suas redes.

Finalmente, entendo como segurança cibernética não só a proteção a dispositivos e dados, mas também a todos os processos e procedimentos envolvidos que possam impactar, de forma significativa, o serviço prestado por um órgão ou instituição. Uma definição mais ampla considera que a segurança do espaço cibernético é importante para garantir, por exemplo, a segurança econômica, dado que empresas oferecem serviços e produtos por esse meio, além das outras esferas da sociedade, que se utilizam de suas tecnologias para possibilitar as mais variadas interações humanas.

Quanto à defesa cibernética, entendo estar mais relacionada a aspectos amplos para a garantia da soberania nacional, integridade territorial e proteção de infraestruturas críticas em certas condições incluindo, por exemplo, a vigilância física sobre cabos submarinos pelos quais redes nacionais conectam-se a outras internacionais, além da avaliação quanto à execução de ações ofensivas de interesse nacional.

---

[48] Texto original: "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

[49] Texto original: "Direct, synchronize, and coordinate cyberspace planning and operations – to defend and advance national interests – in collaboration with domestic and international partners."

2.1.3 Ameaças e ataques cibernéticos

No Brasil, da mesma forma que os conceitos de segurança e defesa cibernética apresentam diferenças conforme o ator que o está definindo, no caso de ameaças e ataques cibernéticos também se percebe uma distinção vista sob a ótica civil ou militar. O Quadro 3 mostra essas diferenças.

Quadro 3 – Definições de ameaças e ataques cibernéticos em documentos do Poder Executivo do Brasil

Termo	Glossário de Segurança da Informação	Glossário das Forças Armadas
Ameaça cibernética	Conjunto de fatores externos com o potencial de causarem dano para um sistema ou organização.	Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.
Ataque cibernético	Ação que constitui uma tentativa deliberada e não autorizada para acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.	Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais em dispositivos e redes computacionais e de comunicações do oponente.

Fonte: Brasil (2021; 2016).

Nota-se que, no caso das Forças Armadas, há o componente ofensivo, já que seria permitida a elas a execução deste tipo de ataque dentro da doutrina e no interesse da defesa nacional (assim como consta na definição de defesa cibernética no mesmo glossário).

Nos EUA, como já dito, a EO 13010, de 1996, definiu as ameaças cibernéticas como "ameaças de ataques eletrônicos, de radiofrequência ou por computador aos componentes de informação ou comunicação que controlam as infraestruturas críticas" (EUA, 1996, n.p.). O dicionário do DoD, de 2011, já define ataques no espaço cibernético (*cyberspace attacks*) como "ações tomadas no espaço cibernético que criam efeitos de negação perceptíveis (ou seja, degradação, perturbação ou destruição) no espaço cibernético, ou manipulação que leva à negação que aparece num domínio físico e é considerada uma forma de disparo[50]"[51] (EUA, 2021, p. 55).

Deibert e Rohozinski (2010) apontam os *riscos* do espaço cibernético para os países, mostrando diferenças entre as ameaças *ao*[52] espaço cibernético e ameaças *por meio*[53] do espaço cibernético. Essa é uma distinção importante porque, com o advento desse novo domínio, as ameaças físicas ainda existem. Não é porque se trata do espaço cibernético que este não sofrerá

[50] O termo disparo é usado porque o termo original, *fires*, é definido como o uso de armas cujos resultados são efeitos letais ou não em um alvo.
[51] Texto original: "Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."
[52] Usando a preposição *to*, indicando que se trata de um alvo.
[53] Usando a preposição *through*, indicando que se trata de um caminho para chegar ao alvo.

efeitos de uma explosão. O fato de ele perpassar o domínio terra já indica que uma explosão pode danificar suas estruturas de comunicação (ou parte delas), seja uma central telefônica, sejam cabos de comunicação, tratando-se de uma ameaça *ao* espaço cibernético. Enquanto isso, a invasão e sabotagem a um sistema computacional consiste numa ameaça *por meio* do espaço cibernético, como o acesso ilegal a sistemas de controle que acionam comportas de uma represa, ou que controlem o espaço aéreo.

Choucri (2012), especificamente sobre conflitos cibernéticos e ameaças à segurança, classificou-os em três tipos mais gerais, de forma a auxiliar seu entendimento e análise. A classificação levou em conta o que mais se percebia à época e, considerando que a tecnologia estava e permanece evoluindo, também considerou somente as ameaças (e proteções, não posso deixar de notar) existentes. O Quadro 4 mostra os tipos definidos e exemplos genéricos de casos.

Quadro 4 – Conflitos cibernéticos e ameaças à segurança

	Tipo	**Casos**
I	Controvérsias acerca da arquitetura e gerenciamento do espaço cibernético	Argumentos fim-a-fim Princípios das camadas Neutralidade da rede "Código é a lei"
II	Conflitos para vantagens políticas e lucro	Poderes estatais para controle político Desafios cibernéticos para o estado Políticas competitivas em foros cibernéticos Crimes e espionagem cibernéticos
III	Ameaças cibernéticas contra a segurança nacional	Militarização do espaço cibernético Guerra cibernética Ameaças cibernéticas à infraestrutura Terrorismo cibernético

Fonte: Quadro 6.1 de Choucri (2012, p. 127, tradução minha).

Apesar de ser uma classificação bem elaborada, ela é insuficiente. Por exemplo, empresas que possuem contratos com governos não podem ter ataques à sua rede e servidores considerados como um *conflito para vantagens políticas ou lucro*, enquanto poderiam ser atos de espionagem. Trata-se de uma *ameaça à segurança nacional*, principalmente se forem empresas da Base Industrial de Defesa, como fornecedores de material e equipamento sensível para armamentos. Em 2015, de James Cilluffo, diretor do *Center for Cyber and Homeland Security* (CCHS), *think tank* da Universidade de Auburn, testemunhou junto ao Subcomitê de Supervisão e Investigação do Comitê de Serviços Financeiros da Câmara dos Deputados dos EUA, e mostrou como atores distintos, com objetivos diferentes, podem executar ataques contra um mesmo alvo e se tratar de um crime cibernético ou uma ameaça à segurança nacional. Por exemplo, bancos podem ser alvo de ataques com fins financeiros (obtenção de dinheiro), ou

interrupção de seu funcionamento (sabotagem) com impacto no funcionamento da sociedade (CILLUFFO, 2015).

O Quadro 2, anteriormente apresentado, utiliza a expressão Ameaças Persistentes Avançadas, do inglês *Advanced Persistent Threats*, cuja sigla APT é mais utilizada. Malloney (2018) define tais ameaças da seguinte forma:

> Uma ameaça persistente avançada é um ataque cibernético dissimulado no qual uma pessoa ou grupo obtém acesso não autorizado a uma rede e permanece não detectada por um longo período. **A definição do termo era tradicionalmente associada com patrocínio estatal**, mas, ao longo dos últimos anos, nós temos visto múltiplos exemplos de grupos não estatais conduzindo intrusões direcionadas para objetivos específicos[54] (MALLONEY, 2018, tradução e grifo meus).

O destaque dado na definição anterior está relacionado à atuação de grupos por países, especificamente, para a execução de ataques cibernéticos com diversos objetivos como espionagem, furto de propriedade intelectual ou mesmo danos a infraestruturas críticas. Um levantamento sobre os APT, incluindo técnicas, ataques atribuídos e outras informações, foi feito pelo ThaiCERT[55], da *Electronic Transactions Development Agency* (ETDA) da Tailândia, primeiramente em 2019. Atualmente, ele conta com uma segunda versão, elaborada a partir de 2020 (THAICERT, 2020), a qual já não é mais um documento PDF, mas um sítio na Internet atualizado com frequência pelo mesmo órgão[56].

A primeira denominação APT dada a um grupo atacante ocorreu no relatório de 19 de fevereiro de 2013, da empresa Mandiant[57]. O relatório estudou uma unidade de espionagem cibernética chinesa, que recebeu o nome de APT1, cujo objetivo era obter propriedade intelectual. O grupo atingiu, à época, 15 países e 141 organizações (VAN PUYVELDE, BRANTLY, 2019; CARLIN, 2018; MANDIANT, 2013, p. 2). Chamo a atenção para o seguinte fato: como as análises das ocorrências são feitas em paralelo por diversos times de *Cyber Threat Intelligence* de empresas, cada uma criou seu próprio padrão de nomenclatura. A empresa Mandiant, por ter criado a sigla APT, desde então nomeia os grupos que identifica com um

[54] Texto original: "An advanced persistent threat is a stealthy cyberattack in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with nation-state sponsorship, but over the last few years we've seen multiple examples of non-nation state groups conducting large-scale targeted intrusions for specific goals."

[55] ThaiCERT é o *Computer Emergency Response Team* (CERT) da Tailândia. A explicação sobre um CERT é dada à frente no texto.

[56] O sítio está disponível em: https://apt.etda.or.th/cgi-bin/aptgroups.cgi. Acesso em: 24 jun. 2024.

[57] A empresa Mandiant foi posteriormente vendida à FireEye em dezembro de 2013, que em junho de 2021 vendeu-a para o Symphony Technology Group. Em março de 2022, a Google finalmente a adquiriu, e ela é, hoje, uma subsidiária da divisão *Google Cloud*.

sufixo numérico. Já a Microsoft nomeia as ameaças com palavras relacionadas com o clima[58], enquanto a empresa CrowdStrike utiliza nome de animais normalmente associados de alguma forma ao país de origem do grupo. Por isso, um mesmo grupo é apresentado com diferentes nomes, cada um batizado por uma empresa quando de sua descoberta e investigação.

Voltando ao Quadro 2, nota-se que a autora identificou várias ameaças cibernéticas, cada uma mitigada de uma forma (DUNN CAVELTY, 2012). No capítulo do livro, ela apresenta as soluções adotadas até o final da década de 1990, as quais evoluíram no decorrer dos anos. É fácil verificar que, antes, havia pouca atuação estatal, quando o domínio do espaço cibernético ainda não era considerado estratégico. Ou, quando era considerado, ainda não havia estrutura estatal para monitorá-lo e protegê-lo. Isso mudou posteriormente com a redação de mais marcos legais e maior envolvimento dos órgãos de forças da lei e dos relacionados à segurança nacional, inclusive na preparação para execução de ofensivas cibernéticas (DUNN CAVELTY, 2012).

Tais ofensivas levantaram a hipótese da guerra cibernética, como advogaram Arquilla e Ronfeldt (1997). Porém, Rid (2017), em seu livro *Cyber War Will not Take Place* afirma já no título que uma guerra cibernética não vai ocorrer. Segundo ele,

> isso significa mais sobre um comentário sobre o passado, o presente e o futuro provável: guerra cibernética nunca aconteceu no passado, não ocorre no presente, e é altamente improvável que atrapalhará nosso futuro. Ao contrário, o oposto é o que tem ocorrido: um assalto à própria violência. Todos os ataques cibernéticos políticos do passado e presente – em contraste ao crime cibernético – são versões sofisticadas de três atividades que são tão antigas quanto o conflito humano: sabotagem, espionagem e subversão[59] (RID, 2017, p. xiv, tradução minha).

Rid (2017), entretanto, vai além. Ele afirma que o uso de ataques por meio do espaço cibernético permite executar, com menor violência, atividades típicas da guerra, quais sejam, sabotagem, espionagem e subversão. Completa ainda, que ataques cibernéticos não se mostraram tão destrutivos quanto um ataque nuclear, conforme se pensou anteriormente, algo que se percebe até hoje. Entretanto, cumpre citar que já houve ataques com sérias consequências no mundo físico. Exemplos: o ataque Stuxnet[60] em 2008, que danificou centrífugas de enriquecimento de urânio na Síria (ZETTER, 2014; WHITE, 2020, pp. 220-246) e a sucessão

[58] A explicação está disponível em: https://learn.microsoft.com/pt-br/defender-xdr/microsoft-threat-actor-naming. Acesso em: 19/06/2024.

[59] Texto original: "It is meant rather as a comment about the past, the present, and the likely future: cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future. Instead, the opposite is taking place: a computer-enabled assault on violence itself. All past and present political cyber attacks — in contrast to computer crime — are sophisticated versions of three activities that are as old as human conflict itself: sabotage, espionage, and subversion."

[60] Também conhecido como Operação Olympic Games, nome original da operação militar.

de ataques à rede de distribuição de energia da Ucrânia em 2015 e 2016, que interrompeu o funcionamento da rede por horas (BUCHANNAN, 2020, cap. 9). Nos dois casos os ataques causaram danos em sistemas SCADA.

Há, na literatura, um caso muito relatado sobre um código malicioso propositadamente inserido em sistemas SCADA, os quais foram furtados pela URSS. Segundo consta, o código sabotado teria causado, em 1982, uma gigantesca explosão em um gasoduto transiberiano (REED, 2004, pp. 268-269). Entretanto, segundo o pesquisador de segurança cibernética Jeffrey Carr, tal explosão se deveu a um erro operacional de um engenheiro e do vazamento de gás, e não a um ataque cibernético bem sucedido (CARR, 2012).

Com relação ao conceito de guerra cibernética, cabe alguns comentários: para Clausewitz (2019, p. 55), a guerra é um instrumento político para atingir os fins, o que é resumido como: "a guerra é a mera continuação da política por outros meios"[61] (CLAUSEWITZ, 2019, p. 55). Na sua definição, na guerra há o componente de violência: "a guerra (...) é um ato de violência para forçar o oponente a realizar nossa vontade"[62] (CLAUSEWITZ, 2019, p. 35).

Voltando à análise de Rid, ele compara *guerra cibernética* com o conceito de guerra para Clausewitz, de modo a demonstrar que aquele não é aplicável, utilizando alguns critérios. Os ataques cibernéticos não têm, necessariamente, um componente violento, típico de guerras. Agressões (cibernéticas ou não), no geral, possuem natureza criminal ou política. No caso de crimes, normalmente seriam ações apolíticas, ao passo que a guerra é sempre uma questão política (como dito anteriormente). No entendimento dele, as ações cibernéticas (cujos objetivos seriam espionagem, sabotagem e subversão[63]) estão localizadas entre os dois polos: natureza criminal e política. Por fim, no caso de crimes, o perpetrador quer ocultar sua identidade, enquanto os militares estariam sempre uniformizados. Ou seja, os perpetradores de crimes e outras ações cibernéticas se utilizam da facilidade de se anonimizar junto ao tráfego de rede, não aparecendo sua própria identidade e origem (RID, 2017, pp. 9-10).

Kello (2017, p. 121) complementa: um programa malicioso (*malware*[64]) não é uma ferramenta efetiva para uma vitória militar (ou seja, não é uma arma tão efetiva), e um ataque cibernético pode parcialmente atingir objetivos táticos. Mas ele afirma que o uso dessa ferramenta pode ampliar o poder militar, sem substituí-lo.

---

[61] Texto original: "War is mere continuation of policy by other means."
[62] Texto original: "War … is an act of violence to compel our opponent to fulfil our will."
[63] As três ações são explicadas mais à frente no texto.
[64] A definição é dada mais à frente no texto.

Já Clarke e Knake (2010) não defendem fortemente o conceito de guerra cibernética. Consideram que o conceito mais importante atualmente é de *resiliência cibernética*, abarcando tanto ações defensivas, quanto ofensivas para o domínio do espaço cibernético (CLARKE, KNAKE, 2019; CLARKE, KNAKE, 2010).

A regra 92 do *Tallinn manual 2.0* do CCDCOE, por sua vez, define ataque cibernético como "uma operação cibernética, seja ofensiva ou defensiva, da qual se espera razoavelmente que cause ferimentos ou morte a pessoas ou danos ou destruição a objetos"[65] (SCHMITT, 2018, p. 415).

Chamo a atenção para o *National Institute of Standards and Tecnology* (NIST) no que se refere a ataques cibernéticos. Os documentos elaborados por esse instituto apresentam definições diferentes conforme o contexto em que são aplicadas: se estão no contexto de tecnologia da informação, de tecnologia de operação, de infraestruturas críticas, de satélites[66]... Traduzo aqui a definição dada dentro do contexto de tecnologia da informação e utilizada por empresas citadas nesta tese: "qualquer tipo de atividade maliciosa que tente coletar, interromper, negar, degradar ou destruir recursos de sistemas de informação, ou a própria informação."[67]

Com relação à utilização de termos como *cyberwar*, guerra cibernética e ciberguerra, Arquilla e Ronfeldt (1997), já em 1997, defendiam em seu trabalho que, como estamos na Era da Informação, o termo mais adequado seria *information warfare*, a ser usado em diversas ramificações na área militar, tanto doutrinárias quanto operacionais. Para eles, à época, o mais importante desse conceito de *cyberwar* seria o objetivo de obtenção de informação (espionagem). Contemporaneamente, contudo, vê-se que os objetivos foram bem mais ampliados.

2.1.4 Diferenças de conceitos entre Estados

É oportuno fazer uma curta observação sobre distinções de conceitos observadas entre países. Quando tratamos de assuntos de pertinência internacional, saber se o mesmo termo ou conceito é entendido da mesma forma por todos os países é importante, por exemplo, quando das definições de normas e nivelamento de estratégias. Betz e Stevens (2011, p. 36) afirmam

[65] Texto original: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."
[66] Todas as definições podem ser lidas nos seus documentos originais disponíveis no sítio do NIST em: https://csrc.nist.gov/glossary/term/Cyber_Attack. Acesso em: 11 jan. 2025.
[67] Texto original: "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself."

que a definição de espaço cibernético utilizada pelo país implica as operações de poder, sendo que isso também aplicado à segurança cibernética. Deibert (2017, pp. 173-174) afirma que a percepção dos governos varia quanto aos "objetos" de segurança cibernética a serem protegidos, e a natureza das ameaças enfrentadas. Ele exemplifica que países de democracia liberal, como os EUA, favorecem redes de comunicação abertas e de fluxo livre de ideias, numa mistura de responsabilidade público-privada, ao passo que países mais autoritários, como China e Rússia, dão maior ênfase à "segurança da informação", o que equivaleria à "segurança do regime", com controles mais territorializados do espaço cibernético.

Deibert (2017, p. 174) também mostra que, de forma aparentemente contraditória, pode-se tratar a *segurança* de uma forma exatamente oposta àquela elencada. A China, com sua presença global também na economia digital, precisa que a rede seja aberta de forma a oferecer seus produtos e serviços, dando inclusive liberdade aos seus cidadãos, o que não ocorre normalmente. E os EUA, com as revelações feitas por Edward Snowden[68], mostraram que são capazes de cooptar empresas e bloquear redes desde que vejam algum risco à segurança nacional ou corporativa.

Alguns países, inclusive, relutam em utilizar o termo *cyber*. O tenente-coronel do Exército dos EUA, Timothy Thomas, estuda guerra informacional (*information warfare*) e é especialista em Rússia. Em 2001 publicou um texto comparando conceitos do pensamento da segurança da informação entre EUA, Rússia e China, chamando a atenção para o fato de eles terem entendimentos distintos. Nos EUA, a segurança da informação e operações de informação não estão dentro da categoria de guerra informacional, ao passo que para a China e Rússia estão. Ou seja, operações cibernéticas podem incluir operações psicológicas o que, nas definições utilizadas pelos EUA, não seria aceitável. Ele conclui, num artigo de 2001:

> O objetivo deste artigo foi examinar o entendimento dos EUA, Rússia e China sobre segurança da informação. O exame mostra que, tanto nas definições quanto na discussão, Rússia e China diferem acentuadamente em sua ideia de segurança da informação à dos EUA. Rússia e a China estão preocupadas com as maneiras de influenciar a mente e as emoções de seus cidadãos. Os EUA, por outro lado, tratam a mente como uma questão separada, governada por diferentes termos: direitos humanos, gestão da percepção e assim por diante[69] (THOMAS, 2001, p. 357, tradução minha).

[68] Edward Joseph Snowden é um cidadão estadunidense que trabalhou na CIA e NSA. Ele vazou, em 2013, documentos oficiais do governo dos EUA, especialmente sobre o programa PRISM, usado para vigilância em massa de usuários da Internet por meio da coleta de seus dados (GREENWALD, 2014).

[69] Texto original: "The purpose of this article was to examine the U.S., Russian, and Chinese understanding of information security. The examination shows that in both definitions and in discussion, Russia and China differ markedly in their idea of information security than does the U.S.. Russia and China are worried about ways to

Destarte, na Rússia o termo “segurança cibernética” seria mais bem entendido como “segurança informacional”, ficando claro que a Internet (e seus sistemas similares) consiste numa ferramenta para tais tipos de ataques. Futter (2018, p. 22) observa o mesmo, afirmando que Rússia e China definiriam “ataques cibernéticos” como “ataques baseados em informações” e incluiriam também ações políticas e psicológicas para desestabilizar governos e influenciar suas políticas. Em outro trabalho semelhante, Giles e Hagestad II (2013) fazem uma comparação entre diversos termos, acrescentando observações feitas em distintas conferências e documentos desde o citado trabalho de Thomas.

A diferença de conceitos entre os EUA, Rússia e China, colocando definições num guarda-chuva de guerra informacional, não está relacionada diretamente a este trabalho. Entretanto, destaco que ela coincide com outras visões como a de Der Derian, de que “[r]ecentemente, a guerra de informação, ou guerra interna, tornou-se o conceito guarda-chuva para guerra cibernética, guerra de hackers, guerra de rede, guerra virtual e outros conflitos centrados em rede”[70] (DER DERIAN, 2009, p. 255, tradução minha).

Essa diferença de conceitos tem impactos significativos tanto na exploração e uso de ameaças cibernéticas quanto, principalmente, na definição de doutrinas e estratégias militares.

Cumpre esclarecer que as definições utilizadas pela Coreia do Norte para os conceitos aqui relacionados não estão disponíveis em fontes abertas.

2.1.5 Capacidades cibernéticas

As capacidades cibernéticas, para diversos países, se tornaram ferramentas de política externa, por exemplo para causar disrupção contra adversários, com um risco mínimo de escalação para um conflito armado (DOMINGO, 2025, p. 265). Como já comentado por Rid (2017), não se trata, necessariamente, de uma guerra cibernética. Entretanto, o domínio é importante de forma estratégica, tendo em vista que é por meio dele que diversas atividades econômicas hoje são executadas e sua disrupção afeta a competitividade entre os países (DOMINGO, 2025, p. 265).

O *Belfer Center for Science and International Affairs*, da *Harvard Kennedy School*, Universidade de Harvard, elaborou, em 2020, um estudo criando o *National Cyber Power Index* (NCPI), o qual foi atualizado em 2022 com pequena diferença metodológica, incremento em

influence the mind and emotions of its citizens. The U.S., on the other hand, treats the mind as a separate issue governed by different terms: human rights, perception management, and so on.”

[70] Texto original: “Recently information warfare, or infowar, has become the umbrella concept for cyberwar, hackerwar, netwar, virtual war, and other network-centric conflicts.”

objetivos e estados analisados (VOO *et al.*, 2022). O índice medido não trata somente de capacidades ofensivas ou de resiliência, mas considera também a participação em negociações técnicas e diplomáticas sobre o assunto, desenvolvimento de competências internamente, além de monitoramento doméstico contra ameaças, inclusive, a outros países (VOO *et al.*, 2022, pp. 4-5). A definição dada para *poder cibernético* (*cyber power*) é "a implantação eficaz de capacidades cibernéticas por um estado para atingir os seus objetivos nacionais"[71] (VOO *et al.*, 2022, p. 7). Em 2010, Nye Jr., pesquisador do mesmo centro e que trabalhou na construção do índice, cunhou a seguinte definição:

> um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador – infraestrutura, redes, *software*, habilidades humanas. Issi inclui não somente a internet dos computadores ligados à rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite. Definindo do ponto de vista comportamental, o poder cibernético é a capacidade para obter resultadors preferidos mediante o uso dos recursos de informação eletrônicamente conectados do domínio cibernético. (NYE JR., 2011, pp. 162-163)

Nota-se que a definição mais recente foi simplificada de modo a, aparentemente, resumir diversos conceitos na expressão "capacidades cibernéticas". No trabalho original de Nye Jr. (2011, pp. 165-173), ele afirma que atores poderiam, por meio do espaço cibernético, exercer tanto poder brando quanto poder duro por meio de diversas formas de ações cibernéticas, conforme as capacidades desenvolvidas.

O *Council on Foreign Relations* (CFR) mantém uma base de dados, chamada *Cyber Operations Tracker*, que registra ações no espaço cibernético notoriamente executadas por Estados[72]. São dados obtidos de fontes abertas e abrangem os anos de 2005 a 2023, contendo 897 operações registradas. Nem todas possuem a identificação da origem dos ataques: 41 não têm origem definida. Entretanto, indicam possibilidades como, por exemplo, que origem em algum país do Oriente Médio ou do Sudeste Asiático, sem que se tenha identificado algum país da região de forma inequívoca.

Izycki (2021) fez um levantamento sobre as capacidades cibernéticas ofensivas de vários países utilizando diferentes fontes. Uma das usadas por ele foi o NCPI de 2020. Neste estudo se utilizou o mais recente, de 2022.

Outro índice relacionado a capacidades cibernéticas é o *Global Cybersecurity Index* (GCI) da ITU. A primeira edição foi laçada em 2015, contando com edições subsequente em

[71] Texto original: "Cyber power is the effective deployment of cyber capabilities by a state to achieve its national objectives."
[72] O sítio pode ser consultado em: https://www.cfr.org/cyber-operations/.

2017, 2019, 2020 e 2024. Seu objetivo é de induzir os países a se preocuparem mais com a segurança cibernética e auxiliar na identificação de oportunidades para melhoria. Nas versões mais recentes (2020 e 2024), o índice quantifica, de 0 a 20, o nível de engajamento dos países considerando cinco pilares: medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidade e cooperação (ITU, 2020; ITU, 2024). Mais à frente utilizo os valores calculados para alguns países de interesse.

Buchanan argumenta, em seu livro *The Hacker and the State*, que as capacidades cibernéticas têm utilidades para os países, como espionagem e sabotagem, mas não serviriam para, por exemplo, sinalizações das posições e intenções de um Estado. Entretanto, oferecem uma versatilidade e certa facilidade para diversas outras ações (BUCHANAN, 2020, p. 307). Kello (2017, p. 123) chama a atenção para o fato de que o espaço cibernético (e as capacidades cibernéticas, por consequência), a princípio, seria um campo para se criar instabilidade política e estratégica. Ele afirma também que, possivelmente, não alteraria de forma significativa a natureza dos conflitos e a balança de poder.

2.2 Regulamentação do espaço cibernético

Há uma literatura extensa sobre a evolução do mundo com o advento da Internet e do espaço cibernético. Da mesma forma, há bibliografia crescente sobre as normas do espaço cibernético e como se inserem na esfera do direito (GOLDSMIT, WU, 2006; LESSIG, 2006) e das relações internacionais (CHOUCRI, 2012; DeNARDIS, 2014; MUELLER, 2002).

Nos últimos anos, muito passou a ser estudado, discutido e escrito sobre a normatização do espaço cibernético. Até a diplomacia, hoje, utiliza expressões distintas para o assunto, dentre os quais destaco dois: Diplomacia Digital (*Digital Diplomacy*) e Diplomacia Cibernética (ou Ciberdiplomacia, do original em inglês *Cyber Diplomacy*). A Organização Não-Governamental (ONG) Diplofoundation (2014) define a primeira como sendo a transformação da diplomacia em três áreas: (i) mudanças nos ambientes políticos, sociais e econômicos em que a diplomacia ocorre, alterando o poder dentro das relações internacionais, originando novos conflitos, incrementando a interdependência ou soberania dos países, dentre outros; (ii) a emergência de novos tópicos a serem colocados nas mesas de discussão diplomáticas, incluindo segurança cibernética, privacidade, governança de dados, comércio eletrônico, crimes cibernéticos e governança da Inteligência Artificial (IA); e (iii) o uso de novas ferramentas na prática

diplomática, tais como mídias sociais, conferências online, análise de dados como *big data*[73] ou usando IA.

Dentro desse arcabouço,

> [a] diplomacia cibernética refere-se à utilização de métodos diplomáticos – negociações, direito internacional e construção de confiança – para lidar com ameaças cibernéticas nas relações internacionais.
> Às vezes, a diplomacia cibernética é usada de forma intercambiável com a diplomacia digital. A prática emergente é que o prefixo ciber seja utilizado quando se considera questões de segurança cibernética, enquanto o prefixo digital seja utilizado para cobertura diplomática de outras questões políticas, como direitos humanos online, dados, comércio eletrônico e conteúdo.
> Globalmente, a diplomacia cibernética é uma ferramenta importante para promover a cooperação internacional e enfrentar os desafios e oportunidades apresentados pelo espaço cibernético. A diplomacia cibernética inclui negociações sobre o cibercrime e a cibersegurança nas Nações Unidas e organizações regionais.[74] (DIPLOFOUNDATION, 2023, tradução minha)

Apesar de a própria definição considerar que esse termo pode ser usado de forma intercambiável com Diplomacia Digital, entendo que se tratam tópicos distintos, os quais têm sido pautados nas mesas de negociação diplomática, principalmente nos últimos anos. Entre as questões sendo discutidas nos ambientes diplomáticos sobre o espaço cibernético, destacam-se, para este trabalho, aquelas relativas à governança, principalmente da Internet, e outras referentes a privacidade, proteção a direitos autorais e crimes cibernéticos.

2.2.1 Governança da Internet

Um histórico simplificado do significado (ou do que pode significar) Governança da Internet pode ser obtido no documento publicado pela DiploFoundation, *An introduction to Internet governance* (KURBALIJA, 2016). Esse documento cita a definição dada pelo Grupo de Trabalho em Governança da Internet (WGIG, do original em inglês *Working Group on Internet Governance*), originado da Cúpula Mundial da Sociedade da Informação (WSIS, do original em inglês *World Summit on the Information Society*) de 2003 e 2005, organizadas pela ITU, ligado às Nações Unidas. A Governança da Internet, então, seria o "desenvolvimento e a aplicação, por governos, pelo setor privado e pela sociedade civil – em seus respectivos papéis

[73] *Big data* é o termo comumente utilizado quando se trata de uma quantidade muito grande de dados.

[74] Texto original: "Cyber diplomacy refers to using diplomatic methods – negotiations, international law, and confidence building – to deal with cyber threats in international relations.
Sometimes cyber diplomacy is used interchangeably with digital diplomacy. The emerging practice is that the prefix cyber, is used for dealing with cybersecurity issues, while the prefix digital is used for diplomatic coverage of other policy issues such as human rights online, data, e-commerce, and content.
Overall, cyber diplomacy is an important tool for promoting international cooperation and addressing the challenges and opportunities presented by cyberspace. Cyberdiplomacy includes negotiations on cybercrime and cybersecurity in the UN and regional organisations."

– de princípios, normas, regras e procedimentos de tomada de decisão, bem como de programas, que devem determinar a evolução e o uso da Internet" (CANABARRO, 2014, p. 128). Tal definição é muito abrangente e cada ator dentro da governança pode ter um entendimento, conforme o papel executado. Como atores, podemos exemplificar os governos, as empresas, operadoras de telecomunicações, provedores de conteúdo, dentre outros (ONU, 2005, p. 4).

A tecnologia de interconexão utilizada pela Internet, como já dito, consiste principalmente na família de protocolos TCP/IP[75]. Dentro dessa arquitetura, uma estrutura é especialmente sensível, sem a qual a rede poderia colapsar mundialmente ou, no melhor caso, funcionar com sérios problemas e impacto regional. Trata-se dos servidores-raiz (em inglês *root-servers*) do DNS. Numa explicação simples, o principal serviço do DNS é prover uma lista de nomes que se converte em números (endereços IP). Conforme explicado mais detalhadamente no APÊNDICE A, cada equipamento ou serviço disponível na Internet possui um endereço IP associado, cabendo ao DNS fazer a conversão dos nomes de domínios ou máquinas[76] em uma sequência de números como 192.168.0.1 (que é tecnicamente mais fácil de uma máquina manipular). Sem essa conversão, vários serviços não funcionam. A mera queda no seu desempenho (demoras na resposta a consultas, por exemplo) pode causar efeitos em cascata em toda a rede. Por ser tão crítico, o serviço de DNS é implementado com redundância, de forma hierárquica e distribuída pela rede e, principalmente nas últimas décadas, com uma maior preocupação contra possíveis ataques cibernéticos.

Outra questão importante é que as respostas dadas pelos servidores têm que ser consistentes, coerentes e coordenadas, com o controle sobre os dados referentes a um domínio ou subdomínio de responsabilidade somente de quem controla seus servidores. Resumidamente, considero domínios como sendo estruturas escritas como *example.com*, *microsoft.com* ou *pucminas.br*. Cada domínio está associado ao menos a um servidor principal e outro secundário para redundância, cujas configurações são de responsabilidade de seus administradores responsáveis.

Outras preocupações desse serviço envolvem, por exemplo, a soberania nacional, dado que cada país é responsável pela administração (ou delegação dessa administração) do seu

[75] Alguns dos principais desenvolvedores na época foram Robert (Bob) Kahn e Vinton (Vint) Cerf, chamados comumente de "pais da Internet". Vint Cerf é uma figura presente até hoje na história e decisões sobre questões de Governança da Internet.

[76] Tais nomes foram criados para facilitar a interação homem-máquina, já que seriam mais fáceis para um ser humano decorar, como *example.com*.

respectivo ccTLD[77], além da atribuição e controle dos domínios de empresas, algo especialmente sensível para aquelas que executam ações comerciais por meio da Internet.

Além dos exemplos citados, há vários outros que envolvem preocupações tão distintas quanto segurança cibernética, direitos autorais, pagamento por meios eletrônicos e questões culturais.

Retornando um pouco na história, na época em que a Internet ainda era um projeto da DARPA com poucos institutos de pesquisa, havia uma quantidade muito pequena de equipamentos computacionais interconectados[78]. A administração dos domínios e endereços IP, assim como a definição das rotas de encaminhamento dos pacotes IP, acontecia de forma manual, sem complicações. Com o crescimento da rede, foi necessário montar um esquema mais robusto sendo que, ainda assim, algumas das solicitações poderiam ser tratadas sem tanta automatização por uma pessoa. Essas funções, que envolviam um misto de atividades administrativas e técnicas, foram, por muito tempo, executadas por Jonathan (Jon) Postel, pesquisador e desenvolvedor do *Information Science Institute* (ISI) da *University of Southern California* (USC). Pioneiro na Internet, Postel começou em 1977, assumindo a administração de nomes e números da Internet, tendo proposto alguns dos primeiros domínios de topo (TLD, do original em inglês *Top-level Domains*)[79] como *.edu*, *.com* e *.net*, além de construir as primeiras versões do protocolo SMTP[80], usado até hoje no envio de e-mails (GOLDSMITH, WU, 2006, pp. 29-33).

Em 1983, a função de administração de nomes e números da Internet executada pessoalmente por Postel (e outros auxiliares posteriormente) passou a receber a chancela "IANA", despersonalizando as atividades, ainda que continuassem a ser executadas por um conjunto mínimo de pessoas. Essas funções de atribuição de nomes e números dentro desse contexto são comumente denominadas "funções IANA". IANA é o acrônimo de *Internet Assigned Numbers Authority* (Autoridade para Atribuição de Nomes e Números da Internet, numa tradução livre) (MUELLER, 2002, p. 92; CANABARRO, 2014, pp. 144-145).

Em maio de 1990, o contrato para o projeto da ARPANET foi aberto para empresas privadas pela primeira vez, tendo assumido a tarefa de administração, principalmente dos

---

[77] *Country Code Top Level Domain*, que consiste no domínio correspondente a cada país, como o .br para o Brasil, .ar para a Argentina e .de para a Alemanha. Tais domínios seguem a lista de códigos de países conforme a ISO 3166-1.

[78] Na verdade, havia um número ínfimo de equipamentos computacionais nos institutos, quanto mais conectados em rede.

[79] Também chamados de domínios de primeiro nível, são os domínios genéricos sobre os quais se criam as regras para se registrar os subdomínios (ou domínios de segundo nível).

[80] *Simple Mail Transfer Protocol*, ou protocolo simples de transferência de correio.

servidores-raiz, a empresa *Network Solutions, Inc* (NSI) (GOLDSMITH, WU, 2006, p. 35). Ainda assim, Jon Postel se manteve como autoridade para definir as políticas (*policies*) dos domínios de primeiro nível, como subcontratado por aquela empresa (CANABARRO, 2014, p. 146; MUELLER, 2002, p. 92). Nesse momento em que, não havendo mais restrição à abertura comercial, possibilitou-se a mistura e integração de redes acadêmicas, comerciais e governamentais, adotou-se o nome Internet a toda essa interconexão de redes.

Com a ampliação das interconexões, maior internacionalização da presença (tanto em termos de pessoas, equipamentos e pontos de conexão, quanto em línguas e sociedades conectadas), a administração dessa governança ficou mais complexa, não só das "funções IANA", mas também na arbitragem de conflitos e interesses estatais distintos sobre qual futuro aquela rede poderia trazer.

Um ator que passa a ter interesse nesse assunto é a Organização Mundial da Propriedade Intelectual (OMPI, ou em inglês WIPO, *World Intellectual Property Organization*). O incremento do uso comercial da Internet atraiu a atenção de empresas que passaram a querer proteger suas marcas, principalmente com o registro de domínios de segundo nível. Tendo em vista que havia, naquele momento, uma empresa responsável pelo registro destes domínios (NSI), era do interesse desta que a busca por domínios aumentasse e que a operação fosse lucrativa, num primeiro momento não necessariamente respeitadora de regras de propriedade intelectual (CANABARRO, 2014, pp. 156-158).

Destaca-se a importância, no contexto da Internet, da *Internet Corporation for Assigned Names and Numbers* (ICANN, numa tradução livre, Corporação da Internet para os Nomes e Números), que consiste legalmente em "[u]ma organização privada, sem fins lucrativos, criada sob as leis da Califórnia, aberta à participação internacional" (CANABARRO, 2014, p. 102) que, desde 1998, funciona "como um fórum pluriparticipativo de articulação política dos diversos atores (estatais e não estatais, técnicos e não técnicos) interessados na formulação das diretrizes relativas à organização, ao funcionamento e à associação à Internet" (CANABARRO, 2014, p. 27).

Outro relevante palco de discussões acerca da Internet é o *Internet Governance Forum* (IGF, Fórum de Governança da Internet), criado pela ONU a partir de 2006, com o objetivo de servir como "um espaço institucional destinado ao diálogo de atores interessados no desenvolvimento do regime internacional próprio para a Internet" (CANABARRO, 2014, p. 184). A primeira proposta era que valesse por dez anos, mas foi renovado e serve como um palco para se discutirem diversos assuntos, com vários atores envolvidos na governança da rede,

e estabelecer pontos de diálogo, sem que um único ator tenha poder decisório sobre quaisquer políticas.

Outras organizações, cada uma com participação especial, mostraram-se importantes no formato da governança como há hoje, como a *Internet Society* (ISOC) e o Consórcio InterNIC. Ambas tiveram parte essencial na construção da ICANN. Suas participações e histórico não serão abordadas neste trabalho, dado que fogem a seu escopo.

O governo Clinton, em 1997, determinou a transição da Governança da Internet, que sairia do controle do governo dos EUA, mas deveria ser feita de modo a evitar o controle por outros governos, tendo em vista a questão estratégica que ela representava. Essa transição ficaria sob responsabilidade da *National Telecommunications and Information Administration* (NTIA), ligada ao Departamento de Comércio do Poder Executivo estadunidense.

> Com o Livro Branco, o Departamento de Comércio ressaltou as seguintes condições para o avanço do processo: i) qualquer nova instituição formada para tomar conta da raiz deveria ser sediada nos Estados Unidos; ii) ela deveria garantir a representação equitativa dos setores interessados; iii) a NSI teria suas atividades, de alguma forma, afetadas e deveria reconhecer a nova entidade como fonte de orientação para as políticas do DNS; e iv) um mecanismo institucionalizado de resolução de controvérsias sobre direitos a nomes seria estabelecido sob os cuidados da Organização Mundial da Propriedade Intelectual (CANABARRO, 2014, p. 162).

Dessa forma, iniciou-se o desligamento dos Estados Unidos como mantenedor e principal determinador das políticas futuras da Internet. No entanto, tal desligamento efetivo não ocorreu até hoje. Na Estratégia Cibernética Nacional dos EUA de 2018, consta o seguinte, na ação "Promover um modelo pluriparticipativo de Governança da Internet":

> Os Estados Unidos continuarão a participar ativamente dos esforços globais para garantir que o modelo pluriparticipativo de Governança da Internet prevaleça contra as tentativas de se criar arcabouços centralizados em estados que poderiam debilitar a abertura e liberdade, dificultar a inovação, e comprometer a funcionalidade da Internet. O modelo pluriparticipativo de Governança da Internet é caracterizado por processos transparentes, *bottom-up*, por construção de consensos e permite a governos, setor privado, sociedade civil, academia e a comunidade técnica participar em pé de igualdade. O governo dos Estados Unidos defenderá a natureza aberta e interoperável da Internet em fóruns multilaterais e internacionais por meio do engajamento em organizações chave como a *Internet Corporation for Assigned Names and Numbers*, o *Internet Governance Forum*, as Nações Unidas e a *International Telecommunication Union*.[81] (EUA, 2018b, p. 25, tradução minha)

[81] Texto original: "The United States will continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet. The multi-stakeholder model of Internet governance is characterized by transparent, bottom-up, consensus-driven processes and enables governments, the private sector, civil society, academia, and the technical community to participate on equal footing. The United States Government will defend the open, interoperable nature of the

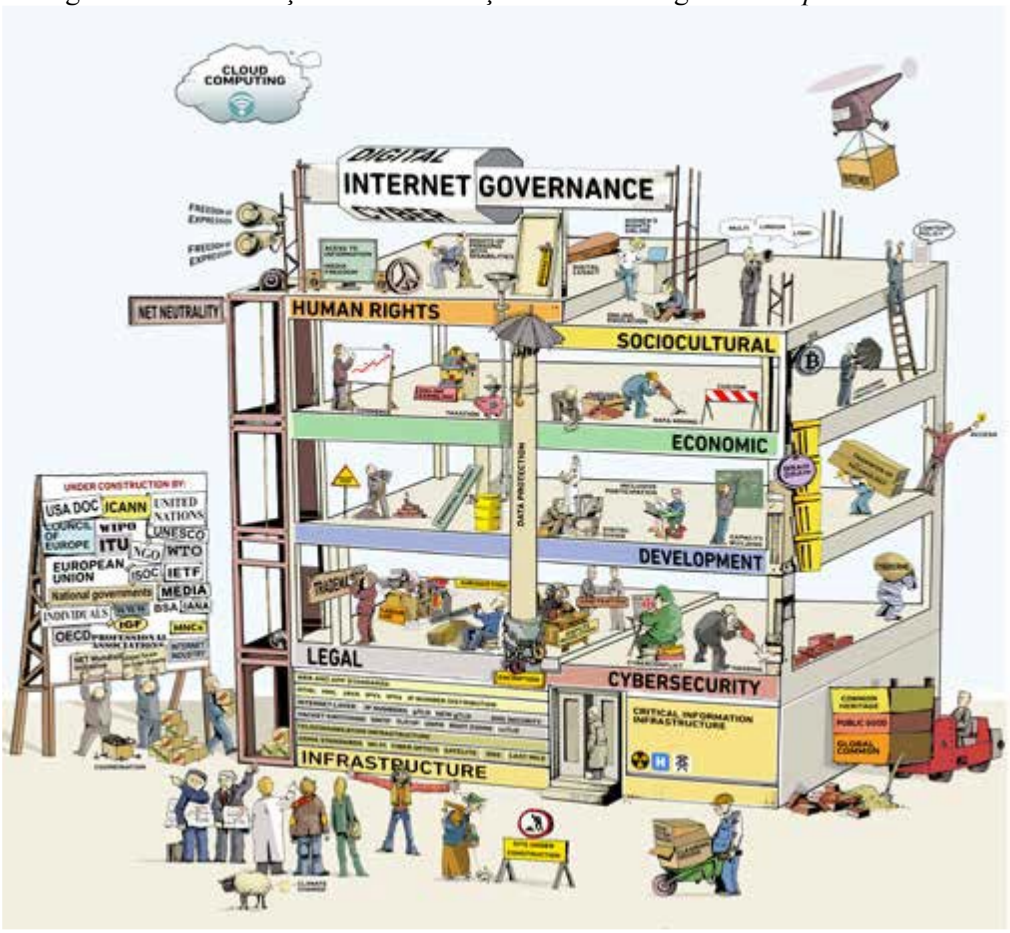
Percebe-se que vários organismos multilaterais são citados (ICANN, IGF, ONU e ITU). Na Estratégia Cibernética Nacional mais recente, de 2023, não se fala especificamente sobre a Governança da Internet, mas se mostra a preocupação com temas técnicos, como o protocolo de roteamento *Border Gateway Protocol* (BGP) e o DNS. No objetivo 4.1 da Estratégia (Proteger os fundamentos técnicos da Internet[82]) consta que o país reconhece a importância estratégica da Internet para si (EUA, 2023a, pp. 23-24).

A Figura 4 ilustra parte da complexidade de se construir essa governança, como apresentada por Kurbalija (2016, p. 29). Essa figura é interessante porque ilustra o que é dito, no mesmo artigo, sobre as "cestas" (agrupamentos) em que os problemas (ou pontos controversos) com relação à Governança da Internet são classificados. As "cestas" que o autor utiliza representam as seguintes características: infraestrutura; segurança; legalidade; econômico; desenvolvimento; sociocultural; direitos humanos (KURBALIJA, 2016, n.p.).

Internet in multilateral and international fora through active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers, the Internet Governance Forum, the United Nations, and the International Telecommunication Union."

[82] Tradução livre de "Secure the technical foundations of the Internet."

Figura 4 – A construção da Governança da Internet segundo a *DiploFoundation*



Fonte: Kurbalija (2016).

Canabarro faz um levantamento de como a Governança da Internet desde o início e como evoluiu ao longo dos anos. Dentre os dados históricos, chama a atenção a mensagem da pesquisadora Avri Doria, do *Lulea Institute of Technology* da Suécia, em uma lista de discussão do *Internet Governance Caucus* (IGC)[83], em 14 de dezembro de 2012, afirmando que "o que distingue a Internet de outras internets é justamente o regime global distribuído de governança que se estabeleceu em torno daquela" (DORIA *apud* CANABARRO, 2014, p. 57). Cabe lembrar que há outras tecnologias de interconexão de sistemas computacionais e, portanto, utilizou-se o termo genérico "internets" para representar as tecnologias concorrentes à da Internet. O mesmo trabalho abrange a institucionalização da Governança da Internet. Essa institucionalização se refere ao "processo através do qual organizações e procedimentos adquirem estabilidade e valor" (HUNTINGTON *apud* CANABARRO, 2004, p. 142).

[83] O IGC seria "uma espécie de 'conferência política' (na tradução de *caucus* para o português) permanente, existente desde 2003, que se presta à articulação de indivíduos dos cinco continentes, representando diversos setores da sociedade civil em sentido amplo, em temas direta e indiretamente relacionados à Internet" (CANABARRO, 2014, p. 31).

Destaco a afirmação de DeNardis, no início de seu livro: "A natureza difusa das tecnologias de Governança da Internet está mudando do controle histórico sobre essas áreas de interesse público de burocracias de Estados-nação para ordens privadas e novas instituições globais"[84] (DeNARDIS, 2014, p. 1, tradução minha).

Para complementar, Lessig[85] (2006) destaca as diversas mudanças ocorridas nesse tempo, com algumas poucas listadas aqui. Interessante reparar o que menciona no início do prefácio para a segunda edição do seu livro *Code version 2.0*, quando afirma:

> Essa é a tradução de um velho livro – na verdade, no tempo da Internet[86], é a tradução de um texto antigo. Ele foi escrito em um contexto muito diferente e, em muitas coisas, foi escrito em oposição àquele contexto. Como descrevi no primeiro capítulo, a ideia dominante entre aqueles que deliravam sobre o espaço cibernético à época, era que o espaço cibernético estava além do alcance da regulação do espaço-real. Governos não poderiam tocar a vida *online*. Portanto, a vida *online* seria diferente, e separada, da dinâmica da vida *offline*. *Code v1* foi um argumento contra essa visão popular.
> Nos anos seguintes essa visão se extinguiu. A confiança dos excetalistas da Internet minguou. A ideia – e até o desejo – de que a Internet poderia permanecer desregulamentada já era.[87] (LESSIG, 2006, p. ix, tradução minha)

Percebe-se que Lessig (2006) praticamente concorda que a visão de Negroponte, apresentada anteriormente, era a preponderante, reconhecendo o quanto estava errada, não havendo mais como, na época da escrita de *Code version 2*, se acreditar nas ideias anteriores.

Como já dito, muito tem sido publicado sobre a Governança da Internet e não é escopo do trabalho fechar uma definição do que se trata. Novamente recomenda-se a leitura do texto de Canabarro (2014), que traz uma parte dedicada justamente à definição semântica do assunto. Para questões históricas e técnicas, sugere-se também o resumo dos primórdios da Internet e da comunicação digital por comutação de pacotes de Kleinrock (2010). O trabalho de Gonzales

---

[84] Texto original: "The diffuse nature of Internet governance technologies is shifting historic control over these public interest areas from traditional nation- state bureaucracy to private ordering and new global institutions."

[85] Lawrence Lessig é um professor que trabalha há anos com questões envolvendo o Direito e a Internet, tendo escrito dois livros interessantes: *Code version 1.0*, em 1999, e *Code version 2.0*, em 2006, uma atualização do primeiro, suja escrita foi inovadora, no sentido de ter sido feita de modo cooperativo com diversas pessoas que submetiam suas sugestões por meio da Internet.

[86] A expressão em inglês no texto original, *Internet time*, é utilizada quando se deseja dizer que, por causa da Internet, os eventos acontecem de forma mais rápida e ágil, devido à velocidade com que as informações circulam e as inovações ocorrem. (Nota do Autor)

[87] Texto original: "This is a translation of an old book—indeed, in Internet time, it is a translation of an ancient text. The first edition of this book was published in 1999. It was written in a very different context, and, in many ways, it was written in opposition to that context. As I describe in the first chapter, the dominant idea among those who raved about cyberspace then was that cyberspace was beyond the reach of real-space regulation. Governments couldn't touch life online. And hence, life online would be different, and separate, from the dynamic of life offline. Code v1 was an argument against that then common view.
In the years since, that common view has faded. The confidence of the Internet exceptionalists has waned. The idea—and even the desire—that the Internet would remain unregulated is gone."

(2016), complementar ao de Canabarro (2014), fez uma análise de como é feita (ou deveria ser) a governança da Governança da Internet.

Ainda sobre esse tema, cabe dizer que alguns grupos técnicos e atuantes no dia a dia, por vezes, ficam à margem da Governança da Internet, incluindo aqueles voltados à atuação na área de segurança cibernética (HINOJOSA *et al.*, 2020, pp. 326-327). É uma boa prática que cada local de trabalho (seja empresa, universidade ou órgão público) tenha um *Computer Emergency Response Team* (CERT, Time de Resposta a Emergências Computacionais, numa tradução livre). Idealmente com pessoal dedicado, o CERT é responsável por atividades como coleta de dados, geração de inteligência e treinamento, voltadas à prevenção de incidentes de segurança. Sua atividade estaria principalmente dentro dos domínios Operação de Segurança, Inteligência de Ameaças, Educação do Usuário e Governança da Figura 3, na página 29.

Outro grupo técnico bastante atuante, e que também faz parte da boa prática cada local de trabalho manter, é um *Computer Security Incident Response Team* (CSIRT, Grupo de Resposta a Incidentes de Segurança, numa tradução livre), com pessoal dedicado, responsável pela atuação célere em caso de incidentes de segurança. O domínio relacionado à atividade precípua deste time é a Resposta a Incidentes, conforme os domínios da Figura 3.

Dentro do Comitê Gestor da Internet do Brasil foi criado o CERT.br[88] (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), que acumula as funções de CERT e de CSIRT nacionais, sendo um ponto focal central para apoiar os demais CSIRT no país e no exterior.

Segundo consulta feita à base de dados de CERT/CSIRT do mundo, mantida pelo *Forum of Incident Response and Security Teams* (FIRST)[89], não há grupo ali cadastrado que represente a Coreia do Norte. Em consulta à lista da APCERT (*Asia Pacific Computer Emergency Response Team*)[90], também não consta representante norte-coreano.

2.2.2 Convenção de Budapeste

A natureza transnacional dos crimes cibernéticos, os quais se utilizam principalmente da Internet, por si só traz a dificuldade de harmonizar as leis criminais e arcabouços que permitam a obtenção e compartilhamento de provas entre países, já que a investigação que ocorre em um Estado pode necessitar de dados informações que estariam sob jurisdição de outro. Tal fato levou a vários esforços na construção de soluções regionais ou unilaterais para

[88] Seu sítio na Internet é: https://cert.br/.
[89] A base de dados está disponível em: https://www.first.org/members/teams/.
[90] A lista está disponível em: https://www.apcert.org/about/structure/members.html.

este problema. Outro aspecto que é levado em consideração é distinguir onde estaria a responsabilidade sobre o ataque cibernético. Se se trata de um crime, é algo afeito à justiça criminal, ao passo que outros estariam mais afeitos à segurança nacional ou de defesa (TROPINA, 2020, p. 148). Acerca dos crimes cibernéticos, um dos normativos pertinentes mais antigos é a Convenção sobre o Crime Cibernético, ou Convenção de Budapeste, assinada em 23 de novembro de 2001.

Em 2004, o Conselho da Europa tomou a iniciativa de, em conjunto com outros parceiros, como Estados Unidos e Japão, construir esta Convenção para incentivar a elaboração de legislações nacionais adequadas aos crimes no espaço cibernético e à integração de forças da lei no combate a esses crimes, além da cooperação e troca de dados e vestígios sobre eles. Ainda que tenha sido escrita no contexto de uma organização regional, foi redigida com participação de Estados fora da Europa e aberta à assinatura de outros países. Apesar de certas limitações e da falta de assinatura, trata-se de um normativo que chegou a influenciar a redação de legislações de países que dele não participam (CHOUCRI, CLARK, 2019, p. 232; TROPINA, 2020, pp. 152-153).

A construção da convenção foi feita de modo a abarcar todas as áreas do crime cibernético, desde a definição destes crimes, até quanto à possibilidade de acordos diretos (MLA, do original em inglês *Mutual Legal Assistance*)[91] e resguardos de atividades investigativas internacionais. Num primeiro momento, houve crítica quanto ao fato de não haver mecanismos de proteção aos direitos humanos quanto ao possível abuso de alguns instrumentos do Direito. Entretanto, a prática mostrou que a aplicação não tem sido problemática quanto a isso (TROPINA, 2020, pp. 152-153). Alguns países, como a Rússia e China, não assinaram a Convenção alegando que violaria o conceito de soberania dos Estados, por exemplo, na coleta transnacional de evidências (TROPINA, 2020, p. 153; HSU, MURRAY, 2014, p. 3; DE BRITO, DE CASTRO, 2021, pp. 50-51, 89-90). A Coreia do Norte também não demonstrou interesse em assinar a Convenção de Budapeste.

No Brasil, tal convenção foi ratificada em 2023 por meio do Decreto 11.491 de 12 de abril de 2023 (BRASIL, 2023a). O texto traduzido da Convenção, ou seja, o decreto que a internalizou, determina que cada país signatário deve tipificar como crime diversas ações

[91] Conforme Fornazari Júnior (2015, p. 221), "[o] auxílio direto em matéria penal (...) constitui um instituto de direito público internacional e de direito processual penal (...) por meio do qual se estabelece o intercâmbio entre países acerca de documentos, provas, atos e medidas processuais constritivas patrimoniais."
Cumpre esclarecer que, por vezes, documentos escrevem MLAT (*Mutual Legal Assistance Treaty*, Tratado de Assistência Legal Mútua, numa tradução livre), sendo que, na realidade, este seria o tratado ou acordo que permite o uso do auxílio direto (MLA) entre dois ou mais países.

relacionadas a computadores e sistemas informatizados, as quais são listadas na Seção 1 - Direito Penal do citado diploma legal. A lista destes crimes é reproduzida no ANEXO A, conforme traduzida e publicada na legislação pátria.

2.2.3 Convenção das Nações Unidas contra o Crime Cibernético

Discussões acerca de um normativo internacional quanto a crimes cibernéticos não são novidade nas Nações Unidas. No relatório A/55/593, emitido pelo Terceiro Comitê de Prevenção de Crime e Justiça em 16 de novembro de 2000, constavam notas sobre a necessidade de um tratado multilateral para o combate a crimes relacionados com tecnologia da informação (TI), à luz de um rascunho que estava sendo elaborado pelo Conselho da Europa, o qual evoluiu para a Convenção de Budapeste. Em 2001, a Assembleia Geral elaborou a resolução A/RES/55/59, designando à Comissão para Prevenção de Crimes e Justiça Criminal a proposição de ações similares para auxiliar no combate a crimes digitais. Entretanto, não houve mobilização e coordenação suficientes para chegar a um resultado semelhante à Convenção de Budapeste. Um dos motivos é que a própria questão de crimes cibernéticos envolve diversas estruturas da própria ONU, como a ITU e a *United Nations Office on Drugs and Crime* (UNODC) e, por vezes, havia questionamentos se um órgão não estaria avançando na competência de outro. Diversas foram as tentativas, mas nenhuma deu o resultado desejado (TROPINA, 2020, pp. 153-155).

A partir de 2019, as Nações Unidas iniciaram nova discussão de um tratado sobre crimes cibernéticos, diante de uma proposta feita primeiramente pela Rússia à Assembleia Geral, com apoio de dezenove outros estados-membros (ONU, 2019b). Dentre os estados proponentes, além da Rússia estavam China e a Coreia do Norte[92], os quais não assinaram a Convenção de Budapeste pelas questões citadas quanto à suposta violação de soberania. Para a discussão do tema, foi formado o Comitê Ad Hoc para Elaborar uma Convenção Internacional Abrangente sobre o Combate ao Uso de Tecnologias de Informação e Comunicação para Fins Criminosos[93]. Uma questão que já se pode observar é a ausência de "crime cibernético" ou "cibercrime" no nome do comitê. De fato, a proposta ampliou o escopo, abarcando todo e qualquer uso de tecnologias de informação e comunicação (TIC) no cometimento de qualquer crime. Neste caso,

[92] Os países que apoiaram a proposta na época foram: Argélia, Angola, Azerbaijão, Belarus, Bolívia, Burundi, Camboja, China, Coreia do Norte, Cuba, Egito, Eritreia, Irã, Cazaquistão, Laos, Líbia, Madagascar, Mianmar, Nicarágua, Rússia, Síria, Sudão, Suriname, Tadjiquistão, Uzbequistão, Venezuela e Zimbábue.

[93] O nome original, em inglês do comitê é "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes."

é possível imaginar uma situação na qual a interceptação de uma ligação telefônica de um narcotraficante estaria contemplada nessa convenção, por exemplo.

O comitê chegou a fazer reuniões frequentes com países, empresas e a sociedade. Alguns questionamentos surgiram nas discussões[94], dentre eles a falta de foco somente nos crimes cibernéticos, ignorando o uso de TIC para outros crimes, e questões de direitos humanos. Diversas posições foram publicadas contra a convenção (HASSAN, 2024; GREIG, 2024), inclusive de ONG como a *Human Rights Watch* (HRW), que foi e continua contra a assinatura (HRW, 2024; BROWN, 2024), a *Electronic Frontier Foundation* (EFF) (EFF, 2024) e a *Privacy International* (PRIVACY INTERNATIONAL, 2024), além de um consórcio de mais de 150 empresas relevantes da área (CYBERSECURITY TECH ACCORD, 2024).

Após os cinco anos que esteve em discussão, e apesar das posições contrárias citadas, a proposta foi aprovada com unanimidade pelos 193 países na Assembleia Geral de 2024. O texto ainda será assinado em uma cerimônia formal, com data a ser definida, em Hanói, Vietnã, em 2025 (ONU, 2024c). O relatório final propôs a adoção do nome de *United Nations Convention against Cybercrime* (numa tradução livre, Convenção das Nações Unidas contra o Crime Cibernético) (ONU, 2024b).

2.2.4 Interpol (ICPO)

A Interpol, cujo nome original em inglês é *International Criminal Police Organization* (ICPO) é um organismo internacional que une polícias judiciárias dos seus países membros. Ela foi fundada em 1923, tem sede em Lyon, França, e conta hoje com 196 países-membros. A própria existência ou história da Organização merece diversas páginas ou mesmo livros. Mas aqui só chamarei a atenção de alguns pontos que se relacionam de modo mais próximo a esta pesquisa.

Primeiramente, a Constituição da organização, em seu artigo 3º, menciona que "[é] terminantemente proibido à Organização realizar qualquer intervenção ou atividade de caráter político, militar, religioso ou racial"[95] (INTERPOL, 2023, p. 3, tradução minha). Essa postura de independência e neutralidade política da organização foi ratificada pela Resolução 04 da Assembleia Geral da Interpol-ICPO, no Rio de Janeiro, em 2006 (INTERPOL, 2006).

---

[94] Todos os documentos elaborados pelo Comitê e suas reuniões estão disponíveis no sítio da UNODC em: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[95] Texto original: "It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character."

A Interpol serve, principalmente, como um ponto de troca de dados e informações de interesse criminal, além de compartilhamento de experiências, tecnologias e técnicas, facilitando a cooperação entre as polícias criminais do mundo. Assim, é um espaço para geração e troca de inteligência, não executando investigações de casos concretos, ainda que haja atividades comuns nas duas atividades. Faz parte também dessa cooperação incrementar o conhecimento através da preparação para atendimento a ocorrências e construção de capacidades para atendimento das mesmas (TROPINA, 2020, p. 151). Seus padrões, quando existem, não são impostos, normalmente consistindo de orientações que facilitam a integração e troca de informações, como já citado.

Relacionado especificamente a crimes cibernéticos, em 13 de abril de 2015 foi inaugurado, em Singapura, o *Interpol Global Complex for Innovation*. Nesse complexo estão duas diretorias: uma para crimes cibernéticos e outra para o centro de inovação, *Innovation Centre*. Dentro deste, há laboratórios por meio dos quais a instituição presta apoio a investigações de crimes cibernéticos, executa treinamentos e dá suporte a polícias na criação de estruturas em seus países (INTERPOL, 2022).

Chamo a atenção para a participação brasileira na organização: o Brasil faz parte da Interpol desde sua fundação, e já contou, de 2010 a 2013, com um policial federal brasileiro no cargo de Diretor Mundial de Polícia Forense, José Helano Marcos Nogueira. Em 2024, outro policial federal brasileiro, Valdecy de Urquiza e Silva Júnior, foi escolhido pelos países componentes do órgão para ocupar a posição de secretário-geral, sendo inclusive o primeiro cidadão do sul-global em tal posto. Além deles, outros seis brasileiros, policiais federais especialistas na área de ciências forenses em crimes cibernéticos, ocuparam (e ocupam) chefias em diferentes diretorias em Singapura[96].

Apesar da importância que a Interpol representa para a resolução de casos criminais, capacitação e troca de tecnologias, a Coreia do Norte não participa dela.

[96] Informação obtida dos Boletins Semanais internos do Departamento de Polícia Federal e consulta direta aos policiais federais nomeados.

3 ATAQUES CIBERNÉTICOS

Conforme já é conhecido, o espaço cibernético, hoje, é um domínio que se mostra importante estrategicamente, inclusive na competição entre grandes potências (DOMINGO, 2025, pp. 265-276). A execução de atividades cibernéticas ofensivas, ou ataques cibernéticos, faz parte do uso que os países fazem desse espaço. Ataques cibernéticos precisam ser descritos em um capítulo à parte porque envolvem alguns aspectos de ordem técnica que merecem ser explicados, ainda que não esgotados, para uma melhor compreensão dos capítulos seguintes. Aqui são apresentados alguns conceitos, como superfície de ataque, e são listados objetivos e tipos de ataques cibernéticos. A atribuição é explicada em uma seção e, depois, exemplificadas algumas políticas de proteção contra os ataques.

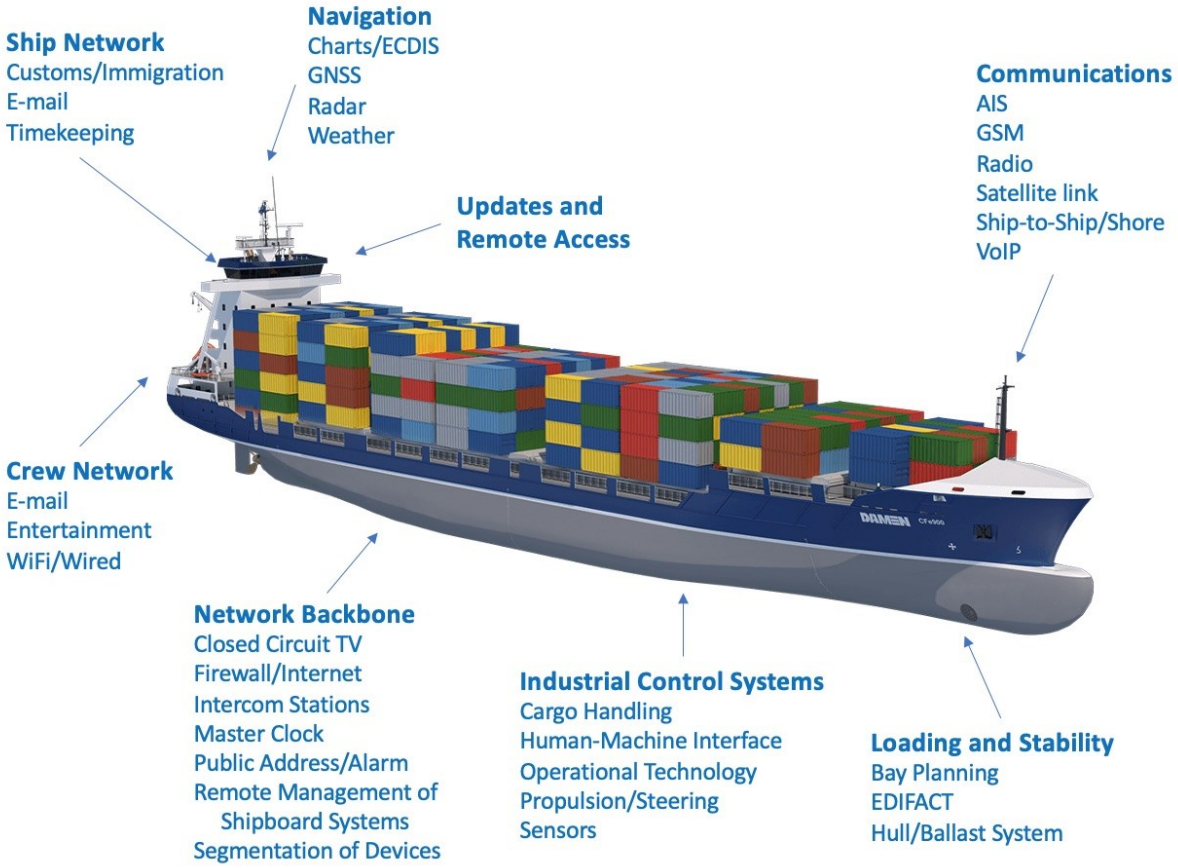
3.1 Superfície de ataque

Quanto maiores as fronteiras terrestres ou marítimas de um país, maior deve ser a preocupação com a defesa de seu território. Quanto maior o corpo de uma pessoa, maior deve ser o escudo ou colete para proteger. Para o espaço cibernético, podemos aplicar um paralelo similar: quanto mais redes possui, quanto maior sua conectividade, quanto mais empresas e instituições estiverem conectadas à Internet, quanto mais equipamentos e sistemas forem acessíveis por meio da rede, maior é o que se chama de superfície de ataque: o conjunto de pontos possivelmente vulneráveis que pode ser explorado em ataques cibernéticos.

De modo a fugir dos tradicionais exemplos de redes domésticas com celulares, televisões, computadores e outros equipamentos, exemplifico algumas vulnerabilidades observadas em um navio mercante, como o apresentado por Kessler e Shepard (2020). No livro, os autores listam os equipamentos e tecnologias que pode haver em uma embarcação, bem como suas redes de comunicação. Cada equipamento, dispositivo e conexão é avaliado quanto à sua segurança e, se apresentar algum risco, este é mitigado de alguma forma. Com relação às redes de comunicação em um navio, exemplifico algumas: conexões que enviam o comando dado pela ponte para os motores e leme, redes de comunicação com as bases na terra (via rádio ou satélite), receptores de sinais de posicionamento e navegação na Terra, como *Global Positioning System* (GPS), meios de recepção de relatórios de alertas e previsão do clima, além de redes para uso pela tripulação e passageiros. Ao chegar e atracar num porto há, também, uma comunicação envolvendo a embarcação e a autoridade portuária para troca de dados alfandegários e solicitação de carga e descarga de produtos, por exemplo. Tudo envolve equipamentos da embarcação conectando-se a outros sistemas. Qualquer ponto apresentado, se

vulnerável e atacado, pode impactar não só na embarcação, mas em todo o sistema de transporte marítimo, o qual, inclusive, é considerado uma infraestrutura crítica. A Figura 5 ilustra algumas possibilidades de redes de comunicação de um navio, para auxiliar na percepção da complexidade desse ambiente.

Figura 5 – Redes de comunicação existentes em um navio mercante



Fonte: Figura 5.1 de Kessler, Shepard (2020).

Pode parecer estranho, num primeiro momento, pensar numa embarcação como um alvo de ataque, mas a preocupação não é nova. Trata-se de um veículo com diversos sistemas, tanto no sentido de tecnologia da informação (TI), quanto no sentido de tecnologia operacional (OT, do original em inglês *Operational Technology*), a qual engloba os sistemas SCADA. Além disso, empresas de transporte marítimo podem, como quaisquer outras, ser alvo de ataques cibernéticos em suas próprias redes corporativas, novamente podendo impactar no sistema de transporte marítimo. Por serem empresas multinacionais, estas possuem escritórios em diferentes países, cada um com sua própria rede local e computadores corporativos, nos quais são instalados sistemas conforme a legislação e necessidade local. Num caso real, a empresa de logística Maersk, com presença internacional, foi uma das mais atingidas pelos ataques da

campanha que ficou conhecida como NotPetya, atribuída a atores russos (GREENBERG, 2019, pp. 198-203). Como curiosidade, o possível incremento no uso de embarcações autônomas é algo que tem levantado novos riscos, questões e preocupações junto a empresas, pesquisadores e trabalhadores da área (LI, 2023).

3.2 Objetivos dos ataques e formas de execução

Guisnel (1999) comenta, sobre o início de uma Internet mais acessível e disponível na década de 1990, que

> ...do conforto da sua casa, com um microcomputador, qualquer um pode ir a qualquer lugar. E já que a maioria dos computadores aos quais o usuário se conecta dificilmente é como o Fort Knox, quase tudo é facilmente acessível, não apenas para indivíduos, é claro, mas também para seus países. E os serviços secretos destes também, muitos dos quais já haviam começado a habitar o mundo sombrio da Guerra da Informação[97] (GUISNEL, 1999, p. 19, tradução minha).

Rid (2013, p. xiv) defende a ideia, válida até hoje, que os computadores permitiram executar, no espaço cibernético, três atividades que fazem parte dos conflitos humanos há anos: *espionagem*, *sabotagem* e *subversão*.

O exposto acima por Gusnel mostra exatamente um exemplo de espionagem. O uso de redes de computadores facilitou a forma de trabalho dos agentes de inteligência na obtenção de dados porque, quanto mais conectado estiver determinado ator, maior a superfície de ataque e mais provável dos seus dados estarem acessíveis. Ainda, a velocidade de transmissão e miniaturização de dispositivos de armazenamento permitem a extração rápida de grandes volumes de dados, bem como seu ocultamento. Antes usavam-se os microfilmes, agora, são os cartões de memória tipo microSD. A espionagem cibernética é correntemente executada por diversos países, tanto para obtenção de informações estratégicas quanto para furto de propriedade intelectual (SANGER, 2018; BUCHANAN, 2020).

A execução de sabotagem, no espaço cibernético, normalmente objetiva enfraquecer ou inutilizar algum sistema ou rede computacional. Causar uma explosão, danificar peças de um equipamento ou até fornecer insumos de menor qualidade podem evitar o funcionamento correto de uma máquina qualquer, reduzir seu desempenho ou diminuir a qualidade do resultado de seu trabalho. Se isso for feito do modo menos violento e mais dissimulado, melhor. A

[97] Texto original: "...from the comfort of one's own home, with a microcomputer, anyone can go anywhere. And since most computers the user hook up to are hardly Fort Knox, almost anything is fairly accessible, not only to individuals, of course, but to their countries as well. And their secret services too, most of which have already begun to inhabit the shadowy world of Information War."

alteração na programação de sistemas computacionais, ou sobrecarga de tarefa nos mesmos, podem conduzir ao mesmo objetivo desejado (RID, 2013).

Por último, a subversão, que se trata de uma tentativa de minar a confiança, integridade e constituição de uma ordem ou autoridade estabelecidas (RID, 2013, p. 116). Neste caso, a coordenação das ações de pessoas que possuam um objetivo comum, como ativistas. O uso de redes sociais para discussões acerca de um tema e cooptação de pessoas para uma causa é uma aplicação do espaço cibernético para este fim. Discussões quanto ao uso deste termo conforme o momento histórico (envolvendo sinônimos como insurgência e terrorismo) fogem do escopo deste trabalho, podendo ser lidas em Rid (2018, pp. 113-138).

Kello (2017, pp. 154-155), especificamente quanto à Coreia do Norte, analisa de outra forma, mais abstrata, e avalia que o país tem três objetivos quando usa suas capacidades cibernéticas: ofensivo, psicológico e, por fim, coerção e político. O uso ofensivo envolve, entre outros aspectos, obter divisas estrangeiras para o país. O uso psicológico envolve afetar a confiança de seus adversários quanto à superioridade de suas bases econômicas e militares. Por exemplo, executam ações de sabotagem que, ainda que não haja um impacto físico, pode afetar a moral do adversário e a percepção quanto à segurança dos seus sistemas. Por fim, o objetivo de coerção ou político está relacionado à obtenção de concessões de interesse do regime.

A forma de execução destas ações varia conforme o ambiente em que se trabalha, e cito alguns exemplos interessantes. Em 1989, Clifford Stoll identificou um invasor no sistema computacional em seu centro de pesquisa, o Lawrence Berkeley National Laboratory (LBNL). Ele se conectou por diversas semanas, sempre buscando arquivos relacionados a projetos dos EUA envolvendo satélites e a defesa de mísseis (projeto Star Wars). Em seu livro *The Cuckoo's Egg*, Stoll relata a investigação, executada auxiliando o FBI e a polícia alemã, até chegar no alemão Markus Hess, que fora recrutado pela KGB[98], órgão de inteligência soviético, tendo invadido a máquina no LBNL a partir de sistemas da Universidade de Bremen, na Alemanha Oriental. Ele e outros dois conterrâneos, que executavam o mesmo tipo de atividade em troca de dinheiro, foram julgados por uma corte alemã e presos, cumprido toda a pena (por volta de dois anos de prisão) (STOLL, 1989).

Um objetivo comum é o financeiro, por exemplo, a obtenção de dinheiro a partir do acesso a contas em bancos e corretoras, seja por meio da Internet aos sítios das empresas ou, mais recentemente, de aplicativos móveis instalados em aparelhos celulares dos clientes. A estes somam-se os furtos de criptoativos em corretoras, como Bitcoin e Ethereum, para citar

[98] O nome original do órgão em russo é *Комитет Государственной Безопасности*, ou *Komitet Gosudarstvennoy Bezopasnosti*. Numa tradução livre seria Comitê de Segurança do Estado.

duas das mais conhecidas. Como já dito, este objetivo é bastante observado em atividades ofensivas executadas pela Coreia do Norte (SCHNEIER, 2018, p. 76; KELLO, 2017, p. 147).

Cito aqui alguns outros termos usados no decorrer do texto. Não se trata de uma lista exaustiva, mas só do que é relacionado ao trabalho aqui apresentado. Um dos mais comuns é *malware*, junção das palavras da expressão *malicious software*. É um conceito genérico que abarca todo e qualquer programa feito contendo alguma função inadequada e, por vezes, criminosa. Conforme o Glossário de Segurança da Informação, este consiste num "*software* malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional." Há diversos exemplos dentro desse conceito, como vírus, *worms, trojans* (cavalos de Troia), *spyware, adware e rootkits* (BRASIL, 2021, n.p.).

O *worm* é uma técnica de propagação de *malware* pela rede, enviando cópias de si mesmo entre as máquinas, explorando vulnerabilidades ou falhas de configuração de programas (BRASIL, 2021).

Os *trojans* são um tipo de *malware* que, assim como os cavalos de Troia, executam funções para as quais foi projetado, mas também outras funções maliciosas, sem o conhecimento do usuário. Por exemplo, um programa que te mostra um vídeo ou proteção de tela, enquanto apaga ou criptografa os arquivos dos dispositivos de armazenamento conectados ao equipamento.

O nome *spyware* é dado àqueles *malwares* que monitoram (espionam) atividades de um equipamento ou sistema, coletando e encaminhando os dados coletados para fora da rede instalada. Alguns tipos de *spyware* são *keylogger*, *screenlogger*, *adware* e *stalkerware*. O *keylogger* captura, armazena as teclas digitadas no teclado do computador e envia pela rede para quem tiver invadido o sistema (função semelhante às das máquinas de escrever elétricas descobertas na embaixada dos EUA em Moscou e no consulado em Leningrado, hoje São Petersburgo, analisadas no Projeto GUNMAN[99]). O *screenlogger*, por sua vez, captura a tela ou pedaços da tela do computador, especialmente quanto o botão do mouse é clicado, útil para se obter senhas de teclados virtuais na tela. O *adware* é usado para apresentar anúncios ao usuário e o invasor coletar comissões do anunciante. Por fim, o *stalkerware* serve para monitorar os usos e passos do usuário do dispositivo, enviando as informações para o invasor (BRASIL, 2021; CERT.BR, 2023).

[99] Para mais informações sobre o projeto, Maneki (2018).

Dá-se o nome de *rootkit* ao conjunto de programas e de técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Ele permite que o invasor mantenha acesso com nível maior de privilégio no sistema em que está instalado (BRASIL, 2021, n.p.).

Um *backdoor* (literalmente, uma porta dos fundos) consiste em "um mecanismo que é inserido no sistema, intencionalmente ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados" (BRASIL, 2021, n.p.).

Os aplicativos tipo *wiper* são aqueles usados para apagar (*wipe*), de forma irrecuperável, todos os arquivos, ou parte deles, dos dispositivos de armazenamento no equipamento invadido.

No *phishing*, o atacante se utiliza de envio de mensagens e, através de engenharia social, convence o receptor a executar certa ação, explorando sua inabilidade de identificar que o conteúdo de alguma mensagem é inidôneo. O nome de *spearphishing* é dado a ataques que são construídos de forma mais direcionada a uma pessoa ou grupo de pessoas. Um e-mail, por exemplo, que ludibria o usuário receptor da mensagem, seja apresentando-se como outra pessoa ou oferecendo alguma oportunidade supostamente imperdível, por exemplo. Não se trata exatamente de uma falha técnica nos sistemas, mas na exploração da percepção da pessoa.

Ataques DDoS (do original em inglês, *distributed denial of services*) são aqueles em que são geradas imensas quantidades de requisições ou mensagens a algum tipo de serviço, muito acima do que sua infraestrutura suporta, inundando-a de requisições e esgotando os recursos do alvo, como capacidade de rede, memória ou processamento. Normalmente, isso leva a algum colapso, até que o ataque seja mitigado e os sistemas, recuperados (BRASIL, 2021; BRASIL, 2016).

Há criminosos que executam o que é chamado de *doxing*[100], ainda sem tradução para português. Essas ações consistem em expor dados pessoais (como documentos, fotos e endereços), por algum meio digital, normalmente redes sociais. Os dados podem ser obtidos tanto de fontes abertas (p.ex., nas mesmas redes sociais), em consultas a bases de dados furtadas e vazadas, invasões a sistemas corporativos ou a computadores pessoais, além do vasculhamento de antigos sítios e fóruns da Internet que podem conter informações comprometedoras. Por vezes, organiza-se um dossiê com as informações compiladas. Seus objetivos podem ser diversos, como constranger pessoas, empresas, protestar ou fazer *cyberbullying* ou *cyberstalking*. O coletivo de *hackers* ativistas *Anonymous* executou diferentes formas de *doxing* enquanto esteve ativo (COLEMAN, 2015; DONOVAN, 2017;

[100] O termo tem origem em *dox*, que no jargão significa documentos (docs).

KASPERSKY, 2020). Com relação ao coletivo, um de seus participantes chegou a ser preso e passou a trabalhar como informante para o FBI. Quando ainda no grupo, sob supervisão da agência, organizou e executou diversos ataques e vazamentos de informações contra sítios do Brasil, Síria, Colômbia, Nigéria, Eslovênia, Grécia, Irã e Paquistão, tanto de empresas quanto governamentais (STUCKEY, BLAKE, 2014).

3.3 Táticas, Técnicas e Procedimentos

Para identificação de atacantes, uma das bases de conhecimento mais utilizada é a que compõe o arcabouço MITRE ATT&CK[101], a qual descreve táticas, técnicas e procedimentos (TTP, do original em inglês *tactics, techniques, and procedures*) de adversários. Ela é separada em três matrizes: uma voltada para ações ofensivas em redes e sistemas empresariais e domésticos, outra para dispositivos móveis e outra para sistemas de controle industrial (ICS, do original em inglês *Industrial Control System*).[102] Na matriz de redes empresariais, são identificadas quatorze táticas, cada uma com um objetivo específico, sob a ótica do atacante, as quais são mostradas no Quadro 5.

Quadro 5 – Táticas de ataque conforme matriz empresarial do arcabouço MITRE ATT&CK

	Tática	**Explicação**
1	Reconhecimento	obtenção de informações sobre redes e/ou sistemas para planejar ações.
2	Desenvolvimento de recursos	aquisição ou desenvolvimento de algum recurso computacional (como um programa) para uso nas operações.
3	Acesso inicial	entrada inicial na rede ou sistema, consistindo na invasão em sentido estrito.
4	Execução	execução de algum vetor de código malicioso no ambiente invadido.
5	Persistência	manutenção do seu acesso à rede ou sistema, ainda que o equipamento seja reiniciado.
6	Escalação de privilégios	obtenção de permissões de acesso mais alto ao sistema ou rede.[103]
7	Evasão de defesa	ocultação no sistema de modo a evitar sua detecção.
8	Acesso a credenciais	obtenção de nomes de usuários e senhas.
9	Descoberta	reconhecimento do sistema ou rede invadidos.
10	Movimentação lateral	acesso a sistemas dentro da rede invadida, muitas vezes para atingir algum alvo específico.
11	Coleta	obtenção de dados de interesse sobre sistemas e configurações.
12	Comando e controle	comunicação com os sistemas comprometidos para fins de controle.
13	Exfiltração	transferência não autorizada de dados.
14	Impacto	manipulação, interrupção ou destruição de sistemas e/ou dados armazenados.

Fonte: elaboração própria com base em Palacín (2021, pp. 90-92).

[101] A origem do nome vem de *Adversarial Tactics, Techniques, and Common Knowledge* (Táticas, Técnicas e Conhecimento Familiar do Adversário, numa tradução livre).

[102] As matrizes completas e diversas informações podem ser consultadas no sítio do projeto, disponível em: https://attack.mitre.org/.

[103] Num sistema computacional, usuários possuem níveis de acesso distintos quanto ao que podem ou não fazer. Que programas ou ações no sistema ele pode ou não executar.

Cada uma das táticas anteriormente listadas é composta por diversas técnicas, as quais podem ser divididas em subtécnicas mais específicas, que descrevem o comportamento do atacante. Cada uma das técnicas, por sua vez, é relacionada a procedimentos identificados em ataques passados (PALACÍN, 2021, p. 92). Um exemplo: na tática de obtenção de acesso inicial a um sistema, pode-se usar a técnica de envio de mensagens de *(spear)phishing*. Essa técnica, por sua vez, pode ser dividida em subtécnicas que especificam como a ação a ser executada é encaminhada ao destinatário: por meio de um anexo malicioso à mensagem a ser aberto pelo usuário, ou de um *link* a ser clicado.

A técnica de *spearphishing* foi utilizada para obter o acesso inicial à rede alvo, tanto no ataque à Sony Pictures Entertainment, quanto no ataque contra o Banco Central de Bangladesh, casos que são um pouco mais detalhados à frente neste trabalho.

Um ataque de espionagem executado na camada física (eventualmente envolvendo questões relacionadas com a camada de enlace) necessita literalmente do acesso físico ao meio de transmissão utilizado para comunicação. Não se trata de algo novo. Interceptações telegráficas e telefônicas existem há décadas e são usadas por órgãos de segurança pública e de defesa, bem como por criminosos. Na Internet, todo o tráfego é de dados, então não há que se falar em interceptar uma ligação telefônica, mas sim de um certo fluxo de comunicação, composto por diversos pacotes, algo muito mais complexo. Por isso, o mais usual é se interceptar todo o tráfego passante por um meio (cabos, fibras ou espectro eletromagnético), filtrando o que se deseja (como a partir da origem, destino e tipo de pacote, por exemplo). A NSA já fez diversas interceptações do tipo, seja diretamente em cabos submarinos utilizados para conexão internacional e intercontinental, seja nos Pontos de Troca de Tráfego (PTT) aonde chegam as conexões oriundas de empresas, ou internamente nas redes de empresas e nos seus *datacenters* (BUCHANAN, 2020, pp. 20-25, 28-30, 57-59). Há relatos de que os equipamentos de mergulho autônomo do navio russo Yantar[104], declaradamente de pesquisa, mas na verdade um navio espião, serviriam para executar interceptação em cabos submarinos de interesse. O navio viaja frequentemente por áreas onde tais cabos passam (SUTTON, 2019; MORTON *et al.*, 2025).

Outro ataque à camada física, envolvendo agora a sabotagem de cabos submarinos, envolve rompê-los por meio do uso, por exemplo, de âncoras jogadas no mar e arrastadas por onde os cabos passam. Isso interrompe a comunicação daquele cabo até que seja consertado. Acidentes podem ocorrer devido a tripulações desleixadas. Entretanto, sempre são levantadas

[104] Informações e ilustrações sobre o navio e seus equipamentos, obtidas de fontes abertas, estão disponíveis em: http://www.hisutton.com/Yantar.html. Acesso em: 13 jan. 2025.

desconfianças, como no caso ocorrido na Alemanha em 2024 (PATERNOSTER, 2024; ASTIER, KIRBY, 2024; MILLER *et al.*, 2025).

O invasor do caso relatado no livro *The Cuckoo's Egg* explorou, remotamente, uma falha em um programa de correio eletrônico instalado no computador alvo. O sucesso da exploração da falha permitiu que fosse aberta uma *shell*[105] no equipamento invadido com nível de privilégio de *root*[106] (STOLL, 1989). A exploração remota de falhas é feita a partir de uma máquina qualquer, por meio da rede, sem acesso físico ao equipamento. Normalmente o que se deseja é executar algum comando ou abrir uma *shell* no sistema, o que dá ao invasor a possibilidade de executar quaisquer comandos no alvo. No caso do acesso no nível de *root*, obtém-se a maior permissão possível, sendo permitido executar qualquer comando e acessar qualquer arquivo.

O caso previamente citado é o exemplo de uma invasão a um sistema computacional que, para ações de espionagem, por exemplo, é suficiente. Entretanto, a partir dessa invasão, outras possibilidades existem. Uma delas é a instalação de um programa *backdoor*, utilizado para que o acesso àquele equipamento seja persistente. Assim, caso se corrija a falha do aplicativo que foi explorada para o primeiro acesso, poder-se-á continuar acessando sistema por meio deste *backdoor* instalado. Utilizando o arcabouço apresentado, seria uma técnica para manter a persistência de acesso ao sistema e rede invadidos.

Em alguns ataques pode haver uma combinação, por exemplo de sabotagem e ganhos financeiros. O primeiro costuma envolver a destruição de dados e o apagamento (muitas vezes de forma irrecuperável) de arquivos, enquanto o segundo envolve a exigência de pagamentos, normalmente em criptoativos[107].

A disrupção e sabotagem no espaço cibernético podem ser executadas por várias formas, como por meio de ataques de negação de serviço do tipo DDoS, os quais sobrecarregam o sistema ou a rede, deixando-o inutilizável.

Além do modelo aqui apresentado, da MITRE, outros modelos utilizados na área de *Cyber Threat Intelligence* são o *Cyber Kill Chain* e o *Diamond Model*. O primeiro foi criado e registrado pela empresa Lockheed Martin, baseando-se no modelo militar *Kill Chain* que define a sequência de quatro passos executados em um ataque contra um oponente. No *Cyber Kill Chain*, os criadores identificaram sete passos de um perpetrador na realização de um ataque

[105] Nome dado ao equivalente a um terminal no qual se digita comandos a serem executados pelo sistema.
[106] O maior privilégio existente no sistema.
[107] Isso se deve a dois fatores: é possível receber o pagamento por ataques executados em qualquer país, e porque os criptoativos são, em parte, difíceis de rastrear.

cibernético (YADAV, RAO, 2015, pp. 439-440; PALACÍN, 2021, pp. 19-20). O outro, *Diamond Model*, foi criado como um primeiro modelo científico de análise de intrusão e operações do adversário. Trata-se de um modelo mais simples que complementava o modelo militar *Kill Chain* (CALTAGIRONE *et al.*, 2013; PALACÍN, 2021, pp. 20-21; TIDMARSH, 2023). Todos os modelos são úteis e podem ser usados de forma integrada (FERAZZA. 2022). Aqui escolheu-se detalhar um pouco mais o MITRE ATT&CK por ser completo, além de fornecer uma base de dados aberta e acessível com os TTP já conhecidos.

3.4 Atribuição de ataques

A atribuição de ataques, ou seja, determinar (de forma inequívoca) quem executou (ou está executando) um ataque não é tarefa fácil. Dentre outras informações, envolve identificar o objetivo do ataque e os TTP utilizados, questões basicamente técnicas. Rid e Buchanan (2015, p. 7) entendem tal ação como uma arte que, embora deva ser embasada em detalhes técnicos, por vezes há informações sutis que podem mudar para onde o dedo apontará. A disponibilidade de informações, uso dos métodos corretos junto à competência técnica, por exemplo, são algumas das questões essenciais. Feita uma análise técnica, forense, pode-se determinar o perpetrador, mas isso não define qual a motivação ou objetivo. Isso tem muito mais nuances do que a parte forense seria capaz de dizer (se é que é capaz) e é de extrema importância. Conhecer o motivo envolve outras questões como o contexto político ou geopolítico em que se encontra. Os autores depreendem que o processo de atribuição na verdade seria, portanto, técnico-político. Outra questão importante quanto à atribuição é a comunicação externa. Tendo em vista que a conclusão (ou parte dela) se deva graças a informações sigilosas de inteligência, pode-se determinar que os culpados não serão indicados para não entregar suas fontes (RID, BUCHANAN, 2015).

Lin (2016) traz outro trabalho bastante completo sobre atribuições no ambiente cibernético, separando em três tipos: atribuição a uma máquina de origem do ataque, a uma pessoa e a um grupo perpetrador específico. Todas são perguntas complexas e nem sempre estão relacionadas (no entendimento do autor, saber quem executou não necessariamente leva ao grupo, por exemplo).

Com relação às análises técnicas de artefatos coletados em ações cibernéticas, o arcabouço da MITRE ATT&CK é de grande valia. A partir do momento que se conhecem quais as TTP que uma operação cibernética ofensiva utiliza, a consulta à base pode fornecer os possíveis perpetradores. No próprio sítio pode-se verificar a lista dos grupos atacantes e as

técnicas e procedimentos já observadas em suas ações[108]. A diferenciação entre eles, muitas vezes, varia com o procedimento utilizado. Por exemplo, muitos grupos usam técnicas de *spearphishing* enviando anexos junto às mensagens. A diferenciação seria o procedimento que utilizam: um deles pode encaminhar anexos em formato PDF de modo a explorar uma falha de segurança de algum programa, enquanto outro envia um arquivo executável e sugere ao usuário executá-lo em sua máquina.

Durante certas situações geopolíticas, a atribuição de ataques fica mais simplificada, como Rid e Buchanan afirmam. Por exemplo, a partir de 2014, com o início da guerra entre Rússia e Ucrânia, alvos ucranianos e seus aliados (incluindo empresas fornecedoras para este país) têm maior chance de receberem campanhas cibernéticas a partir de atores estatais russos (ou contratados por eles) do que de outros países. O conflito se iniciou em 2014 com a ocupação da região da Crimeia por forças russas, aumentado de intensidade em fevereiro de 2022. Durante esse tempo, vários ataques cibernéticos ocorreram, como uso de *malware* contra empresas e ocupação de infraestrutura pela ocupação física e controle de um dos pontos de troca de tráfego de Internet da região, o Simferopol IXP[109] (GILES, 2015, pp. 24-25).

Em 2015 um ataque cibernético executado contra a empresa StarLightMedia, um conglomerado ucraniano de TV, foi feito com o uso de técnicas e ferramentas anteriormente utilizadas e adaptadas por um grupo russo. Além dela, outras firmas também foram afetadas, como sua concorrente TRK, a Ukrzaliznytsia (maior empresa de ferrovias do país) e o principal aeroporto de Kyiv, Boryspil. Em todos os casos os ataques foram destrutivos, danificando de forma irrecuperável a parte lógica dos discos rígidos de seus computadores. Não houve ameaça, pedidos de resgate e, ainda, descobriu-se que os atacantes tinham invadido as redes das empresas e nelas permanecido por diversos meses (GREENBERG, 2019, pp. 28-34).

Em julho de 2017 iniciou-se uma campanha de ataques contra diversas organizações ucranianas, a qual foi denominada NotPetya. Alguns detalhes sobre o ocorrido: o ataque foi disseminado por meio da inserção de um código *trojan* no software de contabilidade MeDoc, utilizado por todas as empresas, inclusive estrangeiras, que negociam e pagam impostos na Ucrânia. Em uma certa data, o *trojan* passou a apagar os dados das máquinas infectadas, deixando-as inutilizáveis (GREENBERG, 2019, pp. 179-183; BUCHANAN, 2020, pp. 288-

[108] A consulta pode ser feita no sítio https://attack.mitre.org/versions/v12/groups/.

[109] IXP é uma abreviação normalmente utilizada para Internet Exchange Points, ou Pontos de Troca de Tráfego de Internet (em português se usa também a abreviação PTT). São locais físicos onde diversas redes (sejam comerciais, públicas ou de pesquisa) se conectam para facilitar a troca de tráfego de Internet entre elas. O fato de haver uma só localidade onde as conexões físicas chegam barateia a infraestrutura e a gestão dos equipamentos, já que a outra opção envolveria a construção de conexões entre cada um dos participantes daquele ponto.

289). Nesse ataque, o país mais impactado foi claramente a Ucrânia, mas houve efeitos em outros, já que qualquer companhia estrangeira que lá operava também foi atingida, como as transportadoras Maersk e FedEx, a construtora francesa Saint Gobain, o grupo de empresas de alimentação Mondelez e a empresa britânica Reckitt Benckiser, todas com danos financeiros substanciais. Além de grandes corporações, pequenos empreendimentos também foram afetados, inclusive hospitais fora do país que tiveram consultas, exames cancelados ou refeitos e cirurgias adiadas (GREENBERG, 2019, pp. 198-203). O impacto financeiro estimado pela Casa Branca foi de US$ 10 bilhões (GREENBERG, 2019, p. 183; BUCHANAN, 2020, p. 289). No início do ano seguinte, cada um dos países dos chamados *Five Eyes* (Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia) soltou nota afirmando que esta era, até então, a mais destruidora e custosa campanha da história, atribuindo-a à Rússia (KOVACS, 2018; BUCHANAN, 2020, p. 304).

Esses dois últimos casos são ataques, como se percebe, direcionados principalmente a empresas ucranianas e, após análises por governos e empresas de inteligência cibernética, foram atribuídos ao APT denominado Sandworm, cujos participantes trabalham no serviço de inteligência militar estrangeira da Rússia, conhecido pela sigla GRU[110]. No caso do último ataque houve o uso de ferramentas da NSA obtidas e distribuídas pelos Shadow Brokers (GREENBERG, 2019, pp. 182-183; BUCHANAN, 2020, p. 290).

Além destes, houve também o ataque a empresas de distribuição de energia da Ucrânia em datas próximas ao Natal, nos anos de 2015 e 2016 (este último denominado Industroyer). Ambos são atribuídos também à Rússia (BUCHANAN, 2020, pp. 187-207; SANGER, 2018, pp. 166-170). Diante disso e do conflito entre Rússia e Ucrânia desde 2014, percebe-se que várias ações cibernéticas ofensivas são executadas dentro do contexto da guerra híbrida entre os dois países (ARNOLD *et al.*, 2024; SOLDATOV, BOROGAN, 2022).

Percebe-se, então, que a atribuição se torna mais simples, não eliminando a necessidade de uma análise técnica robusta dos mecanismos de ataque, o que envolve tanto as estruturas (redes e sistemas) utilizadas como base para os ataques, quanto o tipo de ataque utilizado.

Atribuições equivocadas também podem gerar problemas. Numa sequência de ataques em março de 2013 contra bancos e empresas de notícias da Coreia do Sul, o governo chegou a emitir uma declaração informando que um endereço IP chinês estaria envolvido na ação. Entretanto, não houve uma acusação formal. Após certo tempo, verificou-se que se tratava de uma informação incorreta (SANG-HUN, 2013).

[110] O nome original do órgão em russo é Гла́вное разве́дывательное управле́ние, ГРУ, ou *Glavnoye Razvedyvatel'noye Upravleniye*. Numa tradução livre seria Diretoria Principal de Inteligência.

Há também situações em que as atribuições não ocorrem. Um caso interessante é o denominado Red October pela empresa russa de segurança cibernética Kaspersky. Em 2013, foram encontrados indícios de comprometimento em diversas redes e, com uma análise técnica e histórica, determinou-se que os invasores teriam invadido os equipamentos e permanecido neles por cinco anos, extraindo grande quantidade de arquivos. Na lista de vítimas, a maioria seria de "perfil alto": agências governamentais, embaixadas, instituições envolvidas em pesquisa energética e nuclear, companhias de óleo e gás e indústrias aeroespaciais (ZETTER, 2013). O grupo responsável por esse ataque até hoje não foi identificado.

Grupos também podem induzir uma atribuição errada. Por exemplo, utilizar TTP diferentes dos seus, colocar mensagens dentro do código malicioso em outra língua, ou usar uma situação política como subterfúgio, alterando a percepção do oponente (no caso, quem estaria avaliando a ocorrência para dar a atribuição), de modo que conclua aquilo que o atacante deseja (JERVIS, 1970). Um caso emblemático é o das Olimpíadas de Inverno de 2018, em Pyeongchang, Coreia do Sul. No momento da cerimônia de abertura, dia 9 de fevereiro, um ataque cibernético, que recebeu o nome de Olympic Destroyer, foi executado contra toda a infraestrutura do evento. O acesso à Internet ficou fora do ar, os equipamentos servidores, redes Wi-Fi idem, drones de filmagens não decolaram, ingressos não eram impressos e quem já os tinha não conseguiam autenticar nas catracas para acessarem os locais dos eventos. O ataque de sabotagem tinha semelhanças com o NotPetya, de 2017, atribuído aos russos. Entretanto, se considerarmos a condição litigiosa entre Coreia do Sul e Coreia do Norte, este seria o suspeito usual. Quando da análise dos TTP do caso, técnicas identificadas eram normalmente associadas a grupos russos, mas o código da ferramenta *wiper* utilizada guardava semelhanças com uma ferramenta do grupo norte-coreano Lazarus, enquanto códigos de outras ferramentas aparentavam ser as usados pelos grupos APT3 e APT10, ambos associados ao governo chinês. A partir de uma análise mais criteriosa, um técnico da Kaspersky verificou que um dos vestígios que foi avaliado no código foi forjado[111]. Diante da nova avaliação, determinou-se que era um ataque de falsa bandeira e, por fim, o ataque foi atribuído ao grupo russo Sandworm. A razão do ataque seria mais uma retaliação da Rússia ao Comitê Olímpico Internacional (COI), mais especificamente à Agência Mundial Antidoping (WADA, do original em inglês *World Anti-Doping Agency*), os quais suspenderam o Comitê Olímpico russo por irregularidades identificadas em exames de atletas do país, executados durante as Olimpíadas de Inverno de

[111] Em perícia, o vestígio forjado é aquele produzido por interesse do criminoso, de forma proposital, para iludir o *expert* durante o exame na tentativa de desviar suas conclusões (DE ROSA, STUMVOLL, 2023, p. 95).

Sochi, em 2014, assim como outras irregularidades anteriores, ocorridas desde 2011 (GREENBERG, 2019, pp. 249-259; PERLROTH, 2018).

Outro ataque cuja atribuição nunca foi bem definida é o vazamento de ferramentas ofensivas da *National Security Agency* (NSA) que exploravam falhas de diversos sistemas, principalmente da Microsoft, as quais as empresas não tinham conhecimento e, portanto, não havia desenvolvido correções. O grupo que as obteve identificou-se como Shadow Brokers, ofertando as ferramentas abertamente na Internet para que outros grupos adquirissem. Depois de alguns dias, acabaram por disponibilizar todas gratuitamente. A forma como o vazamento aconteceu não foi esclarecida (RID, 2020, pp. 410-422; SANGER, 2018, pp. 227-230; BUCHANAN, 2020, p. 280; PERLROTH, 2021, p. 350). As pessoas responsáveis pelo grupo e sua origem também nunca foram identificadas pela comunidade de inteligência dos EUA (RID, 2020, p. 421).

3.5 Políticas de proteção cibernética

Atualmente, a segurança cibernética é vista como algo mais holístico e amplo, considerando principalmente uma melhor conscientização de usuários. Especificamente quanto a eles, por vezes se usa a expressão *higiene cibernética* de modo a conscientizar que se trata de algo a ser feito sempre, assim como a higiene pessoal (GOODMAN, 2018).

Cabe lembrar que, conforme Deibert e Rohozinski (2010), Dunn Cavelty (2012) e Clarke e Knake (2019), a Internet é uma mistura de redes e infraestruturas estatais e privadas. Portanto, os autores defendem que a preocupação com a segurança deve ser compartilhada, ou seja, que haja cooperação entre os atores. Dunn Cavelty afirma:

> O espaço cibernético é somente parcialmente controlado por atores estatais. Ao menos nos casos de democracias, o poder neste domínio está nas mãos de atores privados, especialmente do setor de negócios. Muito do conhecimento e dos recursos requeridos para tomar medidas de proteção está localizado fora dos governos. Os militares – ou qualquer outra entidade estatal para este assunto – não possuem infraestruturas críticas (de informação) e não têm acesso direto a elas[112] (DUNN CAVELTY, 2012, p. 151, tradução minha).

[112] Texto original: "Cyberspace is only in parts controlled or controllable by state actors. At least in the case of democracies, power in this domain is in the hands of private actors, especially the business sector. Much of the expertise and many of the resources required for taking better protective measures are located outside governments. The military – or any other state entity for that matter – does not own critical (information) infrastructures and has no direct access to them."

Dessa forma, é essencial o envolvimento de empresas, normalmente entidades privadas, principalmente na proteção de sistemas essenciais como infraestruturas críticas. Novamente, Dunn Cavelty (2012, p. 151) afirma o seguinte:

> Segurança cibernética é e continuará sendo uma responsabilidade compartilhada entre atores públicos e privados. Governos devem manter seu papel na proteção de infraestruturas críticas onde necessário, enquanto determinam como melhor encorajar as forças de mercado a incrementar a segurança e resiliência de redes de propriedade de empresas[113] (tradução minha).

Diversos países contam, hoje, com estratégias e políticas de proteção cibernética bastante interessantes para prevenir e mitigar problemas advindos de ameaças ofensivas, contado com a participação de órgãos públicos, empresas e sociedade civil. Em algumas das políticas é dado bastante destaque na proteção de infraestruturas críticas. Órgãos internacionais, como a ITU, também executam ações de conscientização. Aqui relato, de forma ampla, formas que países adotaram para difundir a preocupação e conscientização sobre a segurança cibernética, tanto para a administração pública, quanto para empresas e usuários.

Nos EUA, a *Cybersecurity & Infrastructure Security Agency* (CISA) promove a conscientização sobre a segurança cibernética, bem como infraestruturas críticas, inclusive para a população em geral. Ela emite normativos, instruções e relatórios sobre ocorrências contemporâneas, conforme troca de informações entre empresas e governos, além de tendências. No país, a investigação de crimes cibernéticos é executada principalmente pelo FBI, recebendo denúncias, orientando cidadãos e empresas afetados por esses crimes por meio do *Internet Crime Complaint Center* (IC3). Estes são alguns exemplos de órgãos que foram estruturados para tentar resolver a demanda crescente de ações no espaço cibernético para proteger a população, as organizações e, em último nível, o país. A CISA também possui uma página em seu sítio da Internet na qual apresenta, no contexto de suas atribuições, informações acerca de ameaças de países vindas da China, Rússia, Irã e Coreia do Norte[114].

O Brasil, em temas cibernéticos, esteve na vanguarda em alguns tópicos como, por exemplo, na elaboração do Marco Civil da Internet em 2014. Outras ações mais recentes que chamam a atenção são, em 2018, a publicação da Lei Geral de Proteção de Dados (LGPD), a criação da Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018a) e a Política Nacional de Segurança da Informação (PNSI) (BRASIL, 2018b); em 2020, a publicação da

[113] Texto original: "Cyber security is and will remain a shared responsibility between public and private actors. Governments should maintain their role in protecting critical infrastructure where necessary, while determining how to best encourage market forces to improve the security and resilience of company owned networks."
[114] Disponível em: https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors.

primeira Estratégia Nacional de Segurança Cibernética (e-Ciber) (BRASIL, 2020); e, em 2023, a instituição da Política Nacional de Cibersegurança (PNCiber) e a criação do Comitê Nacional de Cibersegurança (CNCiber) (BRASIL, 2023b).

No Poder Executivo, o Gabinete de Segurança Institucional (GSI) possui, atualmente, uma Secretaria de Segurança da Informação e Cibernética (SSIC), subordinada diretamente ao Ministro Chefe do GSI[115] que tem, entre suas atividades, a organização da Agência Nacional de Cibersegurança (ANCiber) e a criação de um Gabinete de Gerenciamento de Cibercrises (GGCiber). Ao GSI também compete presidir o CNCiber, composto por membros do governo, da sociedade civil, da academia e do setor empresarial. Entretanto, tal Comitê não tem atribuição normativa e de cobrança quanto à implementação de normas ou políticas de segurança cibernética, seja para empresas, seja para a administração pública, o que supostamente será executado pela ANCiber quando de sua estruturação, para o que não há previsão por depender da sua aprovação no Poder Legislativo. Para uma análise e crítica completa sobre os documentos e a governança da segurança cibernética no país, aquela feita por Hurel (2021) permanece atual.

A transnacionalidade do espaço cibernético e das ameaças nele presentes, determina a cooperação entre Estados. Isso importa na padronização de protocolos técnicos (utilizando fóruns globais de governança, como a ITU e ICANN), e na troca de ferramentas, experiências, normativos técnicos e cooperação de forças da lei (por exemplo, por meio da Interpol) para o caso de crimes, sejam crimes cibernéticos ou que se utilizam do espaço cibernético para sua execução). Normativos técnicos podem ser emitidos, por exemplo, pela *International Organization for Standardization* (ISO, Organização Internacional para Padronização) e posteriormente nacionalizados, ou emitidos por órgãos nacionais como o Instituto Nacional de Metrologia (INMETRO) no Brasil, assim como o NIST faz nos EUA. Esses órgãos podem cooperar também entre si na troca de conhecimentos e padronização, assim como outros órgãos relacionados a processos e métricas específicas a áreas industriais.

Além de crimes como furto de informações pessoais, interceptações de comunicações ou adulteração de dados em sistemas informáticos, para citar alguns exemplos, o uso da Internet por terroristas para troca de mensagens e radicalizar indivíduos também acontece (WEIMANN, 2015). Para reagir a esse problema, é necessária essa cooperação entre países, normalmente por meio de seus órgãos policiais.

[115] O organograma completo do GSI pode ser visualizado em: https://www.gov.br/gsi/pt-br/acesso-a-informacao/institucional/estrutura.

Como exemplo de um organismo regional, trago a Agência da União Europeia para a Cibersegurança (ENISA, do nome original em inglês *European Network and Information Security Agency*, que em 2019 adotou o nome de *European Union Agency for Cybersecurity*)[116], um órgão da União Europeia (UE) que trata de questões consultivas de políticas públicas, como, por exemplo, a elaboração do Regulamento de Cibersegurança da União Europeia. Eles também trabalham junto a empresas, especialistas, academia e público elaborando relatórios e orientações. No relatório sobre tendências de ameaças cibernéticas, lançado em setembro de 2024, foram analisadas ocorrências e TTP, sendo relatados riscos envolvendo atores associados à Coreia do Norte, Rússia, China e Irã (ENISA, 2024).

[116] Sítio oficial: https://www.enisa.europa.eu/.

4 A COREIA DO NORTE

Neste capítulo, apresento parte da história da península coreana e da formação do estado norte-coreano, importantes para entender algumas estruturas governamentais. São relatadas também algumas formas de financiamento do regime norte-coreano, sua posse de armas de destruição em massa e uma breve explicação de sanções aplicadas ao país asiático por organizações mundiais e países relacionados com o tema estudado. Por fim, escrevo um pouco sobre as relações do país asiático com o Brasil.

4.1 A península coreana

Geograficamente, a região conhecida como Coreia está no leste asiático, uma península com aproximadamente 220 mil km² de área, um pouco maior que nosso país vizinho Guiana (que possui cerca de 215 mil km²), e menor que Roraima, o décimo quarto estado em área do Brasil (Roraima tem por volta de 238 mil km²). A península tem a leste o Mar do Japão e a oeste a Baía Coreana do Mar Amarelo. Topograficamente, a leste estão os Montes Taebaek, os quais margeiam a costa e onde estão as maiores altitudes da região (o pico mais alto tem 1.708 m). A oeste, as altitudes são bem mais baixas.

A população coreana é considerada um dos povos mais etnicamente homogêneos do mundo, com poucas minorias étnicas ou linguísticas. Entretanto, não há um consenso sobre a sua origem. Pesquisas linguísticas, relacionadas com a língua coreana, mostram que esta pode ter se originado a partir da Ásia Central, com a população falante migrando há milhares de anos para aquela península e, posteriormente, para o Japão. Já investigações utilizando marcadores de DNA sugerem que os ancestrais chegaram à península vindos da Manchúria e do nordeste da Ásia, ali permanecendo por um longo tempo, com parte dela migrando para o Japão há cerca de 4 mil anos. Registros escritos sobre a Coreia de 2 mil anos atrás sugerem que, durante esse tempo, não ocorreram outras migrações em larga escala (SETH, 2010, pp. 9-10).

Entre o século IV e o ano de 676, dividiu o território da Coreia em três estados: Koguryŏ, Paekche e Silla. Este período foi denominado de *Três Reinos* (SETH, 2010, p. 27). Em 935 a península foi unificada pela dinastia Wang em um só reino com o nome de Koryŏ, dado em homenagem ao reino de Koguryŏ. Esta dinastia dominou o país até 1392, sendo este o momento que pode ser considerado como a origem de uma verdadeira sociedade e etnicidade coreana (SETH, 2020, p. 79). Após a dinastia Wang, sucedeu-se a dinastia Yi (também denominada Joseon), que governou o estado com o novo nome de Chosŏn (ou Joseon), até 1910.

Em diversos momentos de sua história, o país foi invadido e posto como vassalo por impérios que dominavam a região: mongol, chinês e japonês, pagando tributos aos imperadores (SETH, 2020). Uma das invasões mais marcantes foi a ocorrida de 1592 a 1597, quando tiveram seu território invadido pelo Japão, sendo defendido pelos aliados à época, os chineses[117]. Foi nessa invasão que ocorreu uma campanha naval que atingiu centenas de barcos japoneses na qual o almirante Yi Sun-sin apresentou armas e táticas inovadoras, incluindo os "navios-tartaruga", primeiros navios com proteção de ferro, os quais resistiam aos disparos japoneses e atacavam abalroando os navios inimigos com um aríete em sua proa (SETH, 2020, pp. 150-155). O filme O Almirante: Correntes Furiosas, baseado nestes fatos históricos, representa essa época (ALMIRANTE [...], 2014). A principal razão desta invasão ser marcante é que , depois deste evento, a Coreia se fechou à entrada de praticamente qualquer estrangeiro (GRIFFIS, 1881, p. 126).

Em 1876, após negociação entre o rei coreano e representantes do então Império do Japão da Era Meiji, ocorreu a assinatura do Tratado de Amizade Japão-Coreia (ou Tratado de Kanghwa ou Ganghwa), com destaque para o uso da diplomacia das canhoneiras[118] por parte do império japonês. Com isso, a Coreia abriu seus portos a mercadores, principalmente japoneses, terminando seu isolamento (SETH, 2018, p. 29; SETH, 2020, pp. 250-251). Após esse tratado, a China ainda buscou influenciar seu vizinho, orientando-o em reformas da sociedade, enquanto o Japão fazia o mesmo, gerando diversos atritos, até a Convenção de Tianjin, em 1885, quando ambos concordaram, inclusive, em retirar suas forças militares que permaneceram na Coreia por anos (SETH, 2018, p. 30; SETH, 2020).

Entretanto, entre os anos de 1884 e 1894, a China se manteve como maior força influenciadora, até a Primeira Guerra Sino-Japonesa (1894-1895), quando o Japão saiu vencedor e foi assinado o Tratado de Shimonoseki. Este estabeleceu a independência da Coreia, ainda contando com uma influência japonesa, principalmente, mas também um pouco russa e bem menor de outros países ocidentais cujo interesse pela região estava aumentando (SETH, 2018, pp. 31-32).

A década de 1895 a 1905 foi de um incremento na rivalidade russa e japonesa quanto ao domínio sobre a península coreana até que, entre 1904 e 1905, ocorreu a Guerra Russo-Japonesa, terminando com vitória do Japão. Em seguida, a influência do Japão sobre a Coreia

[117] Tal evento faz parte do que é chamado, por alguns historiadores, e *East Asian War* (SETH, 2020, p. 150).

[118] Ou diplomacia do canhão, ou diplomacia canhoneira, originalmente do inglês *gunboat diplomacy*. Trata-se de uma forma de coerção utilizada, inicialmente pelo Reino Unido no século XIX, para projetar poder utilizando sua Marinha, fora do contexto de uma guerra, a fim de defender interesses da sua política externa. Ainda hoje há usos da mesma estratégia de formas distintas (DE SOUZA, 2018).

foi consolidada, em 1910, com a assinatura de acordos diplomáticos, reconhecendo-a como uma colônia (SETH, 2018, pp. 32-33) até o fim da Segunda Guerra Mundial.

Assim, até o final do século XIX, ou seja, até há pouco mais de 100 anos, o povo coreano permaneceu unido, vivendo como um só, isolado dos seus vizinhos. Percebe-se que a razão disso era buscar sua segurança devido às sucessivas invasões dos séculos anteriores. Como Griffis (1881, p. 125) escreveu, isso "explica porque a Coreia foi apropriadamente chamada de "nação eremita""[119], ou "reino eremita" (SETH, 2008, p. 28).

4.2 A criação da Coreia do Norte após a Segunda Guerra Mundial

Em 1º de dezembro de 1943, durante a Segunda Guerra Mundial, foi emitida a Declaração de Cairo, assinada por Chiang Kai-Shek, Franklin Delano Roosevelt e Winston Churchill, a qual reconheceu que a Coreia deveria ser livre e independente (SETH, 2020, pp. 327-328).

Após o fim da guerra e devido a divergências entre as duas principais potências vencedoras, a União das Repúblicas Socialistas Soviéticas (URSS ou União Soviética) e os Estados Unidos, ocorreu uma divisão arbitrária da península, cada parte dominada por um dos dois países. Formavam-se, assim, duas Coreias: uma ocupada no sul do Paralelo 38 Norte pelos Estados Unidos, e a outra ao norte do mesmo Paralelo, pela União Soviética (SETH, 2020, p. 328). Interessante destacar que a separação pelo Paralelo 38 Norte não seguiu nenhuma racionalidade histórica ou geográfica, mas simples conveniência das potências dominadoras: militares dos EUA identificaram que tal paralelo cortava a península em duas partes aproximadamente iguais, mantendo Seul na porção sul (SETH, 2020, pp. 328-329).

Em 1948, a separação da península foi oficializada, com a República da Coreia (Coreia do Sul, ou ROK na sigla em inglês) ocupando aproximadamente 100 mil km² da península, e a República Popular Democrática da Coreia (Coreia do Norte, ou DPRK na sigla em inglês), com aproximadamente 120 mil km². Como referências, a Islândia tem 103 mil km²de área e Portugal 122 mil km², aproximadamente. Comparando com o Brasil, Pernambuco tem área próxima de 98 mil km², o décimo nono estado em tamanho. A Figura 6 mostra as fronteiras dos países e a posição de suas capitais, Pyongyang e Seul.

[119] Texto original: "…explain why Corea has been fitly denominated "the hermit nation.""

Figura 6 – Mapa da Península da Coreia moderna

Fonte: Seth (2020, p. xx).

No mesmo ano de 1948, eleições foram realizadas nos dois países, com Kim Il-sung vencendo na Coreia do Norte (SETH, 2020, p. 337) e Syngman Rhee na Coreia do Sul (SETH, 2020, p. 339). Desde tal separação, os dois países seguiram caminhos bastante distintos. China e União Soviética (posteriormente Rússia) influenciaram o governo da Coreia do Norte na direção de um governo comunista, enquanto Estados Unidos e Japão orientaram a Coreia do Sul numa direção capitalista. Apesar de se tratar de um só povo com uma história milenar em comum, a partir desse ponto seguiram com a população dividida, bem como com regimes e economias completamente diferentes.

A separação da península em dois estados nunca foi algo desejado pela população e, conforme esperado, também não foi bem aceito. Um exemplo disso era a constituição do estado norte coreano de 1948 que declarava Seul como sua capital (Pyongyang era a capital temporária) (SETH, 2020, p. 343). Um conflito era inevitável para alguns especialistas. Entretanto não parece haver uma origem certa para a guerra. A tensão entre as duas potências era clara, mas o palco principal ainda era a Europa. Os EUA não queriam uma Coreia do Norte

forte, nem o comunismo se espalhando pela região, ao passo que a União Soviética queria fortalecer o governo Kim, mas ainda era relutante ao tamanho do auxílio. O exército norte-coreano, com 150 mil homens em junho de 1950, era mais experiente (atuaram na Manchúria durante a guerra civil chinesa) e tinha recebido equipamentos soviéticos pesados. A Coreia do Sul, por sua vez com 100 mil homens, não tinha equipamentos e o suporte estadunidense havia diminuído desde 1949. Diversas escaramuças ocorriam na fronteira ao longo dos anos, iniciados normalmente por oficiais sul-coreanos. Até que, em 25 de junho de 1950, houve a invasão, com o objetivo de uma unificação da península, iniciada pelo regime de Pyongyang com apoio (a princípio sem tropas) soviético e chinês. A invasão pegou a todos (Seul, ONU e Estados Unidos, principalmente) de surpresa (SETH, 2020, pp. 343-346). Considera-se esta a data inicial da Guerra da Coreia, apesar de todos os pequenos conflitos anteriores.

Em 7 de julho de 1950 o conselho de segurança da ONU emitiu a resolução S/RES/82 (1950) que criava um comando militar internacional, liderado pelos Estados Unidos, para intervir na península coreana e expulsar as forças da Coreia do Norte do território da Coreia do Sul. Apesar da presença de outros militares durante toda a intervenção, os EUA foram quem mais aportou militares e equipamentos, bem como assumiu custos da ação (SETH, 2020, pp. 346-347).

No início de agosto de 1950, boa parte do exército sul-coreano tinha se retraído até o perímetro de Pusan (vide mapa da Figura 6) e a guerra estacionou, graças à chegada de tropas dos EUA. Em 15 de setembro houve uma invasão na cidade portuária de Inchon, próxima a Seul, que pegou as forças norte-coreanas de surpresa, as quais ficaram em desarranjo, frustrando suas intenções de unificação. No final de setembro, ao invés de retornar à posição do início da guerra, as forças da ONU, lideradas pelo general Douglas MacArthur e Syngman Rhee passaram à posição de desejarem invadir a Coreia do Norte, também com a justificativa da unificação da península. Em 7 de outubro o Conselho de Segurança das Nações Unidas emitiu uma outra resolução, a S/RES/84 (1950), que vagamente sugeriria haver permissão para a invasão da Coreia do Norte. O comando militar unificado das forças da ONU, então, transpôs o Paralelo 38, agora para unificar a península para domínio do sul. A invasão repeliu as forças norte-coreanas até a Manchúria, com o presidente Rhee chegando a visitar Pyongyang, em 20 de outubro, para demonstrar vitória (SETH, 2020, pp. 347-348).

Neste momento, a China enviou militares voluntários, de forma não oficial, para apoiar as forças norte-coreanas, entrando de forma discreta a partir de 19 de outubro. General MacArthur fez uma última ofensiva para tentar finalizar a conquista em 24 de novembro, mas três dias depois sofreu um contra-ataque das forças chinesas recém-chegadas. Em 6 de

dezembro, Pyongyang foi reconquistada, e em mais duas semanas, quase todo o território norte-coreano também. Seul foi de novo invadida, agora pelas forças de apoio chinesas, em 4 de janeiro de 1951 e somente em 15 de março a capital sul-coreana seria retomada. Há diversos relatos de atrocidades executadas pelas forças invasoras, tanto do Norte quanto do Sul, que marcaram toda essa época (SETH, 2020, pp. 348-349).

As conversas para armistício e paz na península se seguiram, incluindo negociações para trocas de prisioneiros. Apesar disso, conflitos ainda continuaram pelos anos seguintes, incluindo bombardeios contra cidades, inclusive Pyongyang, contra represas de água, causando destruição de diversas plantações de arroz e também contra infraestrutura. No total, mais bombas foram jogadas sobre a Coreia do Norte do que sobre a Alemanha ou Japão durante a Segunda Guerra Mundial (SETH, 2020, pp. 349, 356, 364).

Importante destacar o uso de armas químicas como *napalm* durante as campanhas (SETH, 2020, p. 356) e que, em momentos críticos, precisamente durante o ano de 1951, os EUA chegaram a ameaçar o uso de armas nucleares sobre a Coreia do Norte. Tais armas, inclusive, foram posteriormente mantidas pelo governo estadunidense na Coreia do Sul entre janeiro de 1958 até o fim de 1991 (KILCULLEN, 2020, p. 33).

Em 27 de julho de 1953 houve a assinatura de um armistício que vigora até hoje, não havendo um efetivo fim da guerra com a assinatura de um tratado de paz (SETH, 2020, p. 353; KIM, 2020).

A divisão da península coreana após a Segunda Guerra Mundial foi o típico resultado de um novo mundo bipolar, fragmentado em polos de influência bem definidos: os EUA e a URSS disputando a balança de poder global. No caso, a Coreia do Sul recebeu forte influência dos Estados Unidos e outros países europeus, vencedores da guerra, enquanto a Coreia do Norte se manteve sobre a influência principalmente da União Soviética, posteriormente Rússia, e da China, dois países de governo comunista. Como a URSS não se envolveu com o envio de tropas, somente com informações de inteligência e equipamentos, a influência sobre a Coreia do Norte ficou mais a cargo da China durante a Guerra da Coreia (SETH, 2020, pp. 353, 356).

Com relação à economia, após a Segunda Guerra Mundial, o governo da Coreia do Norte soube se beneficiar da disputa entre China e URSS pela influência comunista no País, extraindo apoio de ambos. No caso da China, houve uma relação muito próxima, com acordos bilaterais econômicos e suporte na reconstrução do país após a Guerra da Coreia. Isso incluiu, por exemplo, o perdão da sua dívida externa pelo governo de Mao Tsé-tung e a capacitação da sua população, permitindo que a Coreia do Norte se mostrasse um sucesso econômico maior que a Coreia do Sul até a década de 70 (PACHECO-PARDO, 2014, p. 93).

A integração técnica diminuiu após a Revolução Cultural de Mao e a adoção da ideologia *Juche* (ou *Zuche*) por Kim Il-sung, traduzida com "autossuficiência", a qual consiste, simplificadamente, na ideia de que o povo norte-coreano deve ser nacionalista, politicamente independente e autossuficiente econômica e militarmente (SETH, 2020, p. 372; VISENTINI *et al.*, 2018, p. 83). Supostamente de origem Marxista-Leninista, de acordo com os documentos norte-coreanos, o historiador Michael Seth afirma que "[n]a realidade, é mais um ultranacionalismo vago e glorificação do líder do que uma ideologia sistemática, pouco a ver com o marxismo"[120] (SETH, 2020, p. 372, tradução minha). Resta também dizer que o nacionalismo citado não se trata de um nacionalismo voltado ao povo coreano, mas uma ligação com o novo país que se formava (VISENTINI *et al.*, 2018, p. 84). Além disso, a ideologia passou a pregar o culto à personalidade dos que governam e, portanto, inicialmente a Kim Il-sung e depois aos que o sucederam (VISENTINI *et al.*, 2018, p. 85).

Após a morte de Kim Il-sung, em 1994, o regime lançou a política nacional *Songun*, baseada e complementar à ideologia *Juche*, que significava "Forças Armadas em primeiro lugar", reforçando o nacionalismo e a autonomia, fortalecendo o país (VISENTINI *et al.*, 2018, pp. 146-147). "A nova política significava a elevação do *status* das Forças Armadas, que passaram a ocupar o centro do sistema político norte-coreano e a influenciar amplamente todos os setores da sociedade." (VISENTINI *et al.*, 2018, p. 147). Essa nova política, portanto, justificaria os gastos militares (e com os militares) de qualquer tipo sobre os demais, assim como ações militares sobre o próprio povo.

Dado esse histórico e suas políticas, a Coreia do Norte ocupa uma posição *sui generis* no mundo. Sendo uma espécie de pária no ambiente internacional, ela utiliza diversas formas para obter dinheiro de modo a sustentar seu governo e projetos militares, com Kim Jong-un seguindo a política *Byungjin* iniciada por seu avô e continuada por seu pai, a qual significa "desenvolvimento paralelo". No caso, desenvolvimento paralelo da defesa nacional (construindo um sistema de dissuasão com armamento nuclear e mísseis) e modernização das capacidades econômicas (CHEON, 2013, p. 1; VISENTINI *et al.*, 2018, p. 189). Uma das linhas-guia da política envolveria, inclusive, resolver questões energéticas do país por meio de uma indústria de energia nuclear independente, simultaneamente ao desenvolvimento de suas capacidades nucleares (CHEON, 2013, p. 2). Ainda que posteriormente, em 2018, a política tenha mudado para uma mais focada na economia que nas armas (CARLIN *et al.*, 2022), percebe-se a importância dada ao desenvolvimento de um arsenal militar nuclear para o país

[120] Texto original: "In reality it was more vague ultranationalism and glorification of the leader than a systematic ideology, and it had little to do with Marxism."

que, estima-se, possui 50 ogivas nucleares prontas e tenha produzido material físsil para 90 (KRISTENSEN *et al.*, 2024).

É sabido que esse tipo de política necessita de muito dinheiro e a Coreia do Norte não disponibiliza os dados sobre o PIB e gastos do país. Assim, Estados e ONG estimam tais valores, presumindo-se que a Coreia do Norte gaste 35% do seu PIB com os militares, sendo aproximadamente 6% para as armas nucleares. Para 2023, o gasto total estimado com tais armas foi de US$ 856 milhões (ICAN, 2024, p. 15).

Uma das formas de conseguir divisas é por meio de atividades ilícitas, as quais são bastante conhecidas dentro dos ambientes de política externa, com analistas afirmando, inclusive, que o país apresenta uma "soberania criminal"[121], já que limites impostos pelo Direito Internacional ou legislações de outros países não constrangem a Coreia do Norte, que ainda se utiliza da estrutura governamental para executá-las, incluindo o uso de missões diplomáticas no exterior (KAN *et al.*, 2010, p. vii). Internamente, o governo delega a execução desta política, desde 1974, ao *Central Committee Bureau 39*[122] do *Korean Workers' Party* (KWP, traduzido como Partido dos Trabalhadores Coreanos), único partido do país (KAN *et al.*, 2010, p. 1-2). Outras fontes, entretanto, citam o *Bureau 39* como sendo uma estrutura do governo norte-coreano, sem citar se estaria subordinado ao KWP.

Cumpre dizer que o estudo que sumarizou tais atividades ilícitas foi executado em 2010 no governo de Kim Jong-il, falecido em 17 de dezembro de 2011, mas elas continuaram no governo de Kim Jong-un, seu filho, que assumiu o posto de Líder Supremo da Coreia do Norte no mesmo dia da morte do pai. Entretanto, foi justamente Kim Jong-il que organizou, na década de 1970, o *Bureau 39* para executar ações do seu interesse e ter uma base a seu favor dentro do partido. Ela possui dois ramos: um relacionado a atividades ilegais, e outro a atividades legais (ou aparentemente legais) por meio de empresas, incluindo bancos, sob sua coordenação, com sede em países como Hong Kong, Macau, China e Áustria, restaurantes e até a administração de um museu no Camboja. Para se ter um exemplo da importância desse órgão, ele é responsável pelo monopólio do comércio de minerais do país (SOLOMON, CHI, 2003; KIM JONG-IL'S [...], 2018; BUREAU 39; ONU, 2019a; BURGIS, 2015). As empresas sul-coreanas de eletrônicos LG e Samsung chegaram a comprar ouro norte-coreano, para usar na fabricação de componentes, e, possivelmente, todos os 200 milhões de dólares desta compra foram para contas do *Bureau 39*. Em 2003 estimava-se que haveria US$ 5 bilhões espalhados por diversos

[121] Tradução de *criminal sovereignty*.
[122] O nome varia entre os documentos estudados entre *Bureau 39*, *Office 39*, *Division 39* e *Room 39*. Neste documento utilizo *Bureau 39*.

países sob controle de empresas relacionadas a esse órgão (SOLOMON, CHI, 2003), o qual, cumpre dizer, não é reconhecido oficialmente pelo governo da DPRK (BUREAU 39, 2020).

4.3 Financiamento das atividades do Estado

O financiamento da Coreia do Norte via obtenção ilegal de divisas pelo país é objeto de pesquisas acadêmicas, relatórios governamentais e tema de reportagens investigativas. Relatórios elaborados pelo *Congressional Research Service* (CRS) do congresso estadunidense relacionam várias atividades ilícitas para obtenção de dinheiro (PERL *et al.*, 2007; WYLER, NANTO, 2008). Louise Shelley, uma das pesquisadoras da área de fluxos financeiros ilegais, sumariza vários estudos que, para o caso em tela, mostram os modos "alternativos" de obtenção de divisas pela Coreia do Norte, como fabricação e distribuição de cigarros falsificados, fabricação e distribuição de drogas, como metanfetaminas, e comércio de artefatos da vida selvagem (SHELLEY, 2018, p. 62; GREITENS, 2014; KAN *et al.*, 2010; PERL, 2004; PERL, 2007).

Os registros de tráfico humano envolvendo cidadãos do país são vários, para diversos tipos de atividade laboral, mas percebe-se uma prevalência de atividades braçais como construção civil, estaleiros e trabalhos fabris em confecções. Recentemente foram publicadas investigações relacionadas a uma suposta exploração de trabalho escravo de norte-coreanos em fábricas na China, onde sofrem diversos tipos de abuso pelos seus chefes, também norte-coreanos (PACHECO-PARDO, 2014, p. 105; NORTH Korea's Secret [...], 2018; URBINA, 2024; BUREAU 39, 2020). Não se trata de um caso isolado, dado que isso ocorre também com trabalhadores norte-coreanos em países tão diversos como China, Rússia, Polônia, Mongólia, Catar, Uruguai, Mali e Emirados Árabes Unidos. Essa exportação de mão de obra aumentou nas últimas duas décadas, apesar das sanções impostas pela ONU (BREUKER, 2023, p. 644; NORTH Korea's Secret [...], 2018). A Fundação Walk Free[123] estima, de forma conservadora, que um em cada dez trabalhadores na Coreia do Norte esteja sujeito a situações análogas à escravidão, o maior valor entre os países do mundo (WALK FREE, 2023).

Outra forma der obtenção de divisas que teve alguma repercussão é a falsificação de notas de cem dólares, comumente chamadas no meio de *supernotas* (BUREAU 39, 2020; SHELLEY, 2020; KAN *et al.*, 2010; ONU, 2023; WYLER, NANTO, 2008).

Sob promessas para cumprimento de acordos, o país também recebeu dinheiro estrangeiro de outras formas. Entre 1998 e 2008, foi criada pelo presidente da Coreia do Sul,

[123] Sítio na Internet: https://www.walkfree.org/.

Kim Dae Jung, a política *Sunshine* (Luz do Sol, numa tradução livre) para melhorar as relações bilaterais. Essas ações incluíram, por exemplo, encontros de famílias separadas entre os dois países e o desfile conjunto de ambos nas Olimpíadas de Sydney em 2000 (SETH, 2020, pp. 474-475). Por meio desta política, nesse mesmo ano foi organizada uma cúpula entre os países (o país do sul já governado por outro presidente, Roh Moo-hyun) e foram enviados US$ 8 bilhões em assitência econômica. Investigações posteriores descobriram que quinhentos milhões de dólares foram dados a Pyongyang, pelo Grupo Hyundai, para ter direito à execução de projetos no país, e o mesmo grupo pagou diretamente a um dos responsáveis pelas negociações no governo de Kim Dae Jung grande quantidade de dinheiro. Tais denúncias de corrupção enfraqueceram a política, que também não apresentou os resultados de integração desejados, só a cessão de dinheiro ao governo norte-coreano e à família do ditador (SETH, 2020, pp. 506-508; LEE, 2004, p. 135; TERRY, 2021).

O dinheiro não serve só ao financiamento do Estado, mas também para sustentar os luxos da família Kim e da elite do governo norte-coreano (PERL *et al.*, 2007; WYLER, NANTO, 2008).

Outras formas de obtenção de divisas, relacionadas com o espaço cibernético ,envolvem o furto e lavagem de dinheiro, incluindo criptoativos, e mão oferta de obra especializada para empresas que desejam trabalo remoto. Estes são discutidos com um pouco mais de profundidade no próximo capítulo.

4.4 Armas de destruição em massa

No início do desenvolvimento do programa de armas de destruição em massa (ADM), a Coreia do Norte contou com a capacitação de seus cientistas a partir de um acordo firmado entre seu *Atomic Energy Research Institute*, fundado em 1952, com o *Joint Institute for Nuclear Research* soviético. O acordo foi assinado em fevereiro de 1956 e, com o auxílio da URSS na década de 1960, finalizaram a construção de sua primeira usina e seu primeiro reator nucleares em Yongbyon. O desenvolvimento seguiu internamente, e na década de 1970 adquiriram tecnologia soviética para reprocessamento de plutônio. No ano de 1985 o país assinou o Tratado de Não-Proliferação Nuclear (TNP), exigência para que os soviéticos pudessem repassar aos norte-coreanos a tecnologia de reatores de água leve. Tal assinatura permitiu a fiscalização das instalações do país pela Agência Internacional de Energia Atômica (AIEA), que por vários anos encontrou diversas inconsistências. Informações de inteligência davam conta de que o país estaria aperfeiçoando o reator de Yongbyon, construindo outro, reprocessando o combustível utilizado para deixá-lo em grau de armamento e testando altos explosivos (SETH, 2020, pp.

467-480; TERRY, 2021; LANGEWIESCHE, 2007, pp. 172-176; NORTH Korea's Nuclear [...], s.d.).

Intermediado pelo ex-presidente Jimmy Carter, em 21 de outubro de 1994, Kim Jong-il assinou, com o governo Bill Clinton, o *Agreed Framework*, em Genebra. O objetivo era frear o desenvolvimento do programa de energia nuclear norte-coreano e manter a península coreana sem armas nucleares, além de apoiar a Coreia do Norte na recuperação de sua economia, em crise desde 1980[124]. No acordo constava a garantia de que a Coreia do Norte se manteria no TNP e daria condições para que inspetores da AIEA fiscalizassem suas instalações. Em troca, receberia, dentre outras vantagens, o equivalente a dez anos de petróleo e auxílio no desenvolvimento de uma usina nuclear com dois reatores de água leve. O país, no entanto, sempre questionou que algumas das condições do acordo de 1994 não estavam sendo seguidas, como o investimento sul-coreano, estadunidense e japonês na usina citada, só iniciado em 1999[125], e o fornecimento de petróleo que sempre atrasava. Pyongyang chegou a interromper o desenvolvimento nuclear utilizando plutônio, mas continuou desenvolvendo sua tecnologia de mísseis, ampliando seu alcance, e trabalhando secretamente com o Paquistão e A.Q. Khan no enriquecimento de urânio (SETH, 2020, pp. 467-480; TERRY, 2021; LANGEWIESCHE, 2007, pp. 172-176; NORTH Korea's Nuclear [...], s.d.).

A notícia sobre o enriquecimento de urânio, com base em análises de inteligência, levou o presidente George Bush, em 29 de janeiro de 2002, a classificar a Coreia do Norte como um dos países do "eixo do mal"[126] no seu *State of the Union*[127]. Questionado pelos EUA em outubro de 2002 quanto ao cumprimento do acordo, o país admitiu ter continuado a desenvolver armas nucleares. Em dezembro do mesmo ano expulsou os técnicos da AIEA de seu território. Em 10 de janeiro de 2003 retirou-se do TNP e declarou oficialmente possuir armas nucleares. Em 4 de julho de 2006 a Coreia do Norte lançou sete mísseis sobre o Japão. Por falta de interesse em uma crise com a Coreia do Norte, os países vizinhos não retaliaram. O primeiro teste nuclear foi executado em 8 de outubro de 2006. Em 2007 a Coreia do Norte concordou em parar seu programa nuclear e aceitou o retorno dos agentes da AIEA. Diversos momentos se sucederam, entre abertura e fiscalização pela AIEA[128], expulsão dos técnicos, novos testes nucleares e de

[124] O texto do acordo está disponível em https://peacemaker.un.org/node/9207. Acesso em: 12 jun. 2024.
[125] Na verdade, uma empresa, a KEDO, foi formada em 15 de dezembro de 1999, mas a construção da usina só iniciou em 7 de agosto 2002 (NORTH Korea's Nuclear [...], s.d.).
[126] O termo original usado no inglês foi *axis of evil* e incluía também Irã e Iraque.
[127] O *State of the Union* é um discurso que tradicionalmente o presidente dos EUA dá perante o Congresso no início do ano.
[128] Um bom histórico dos eventos envolvendo a AIEA e Coreia do Norte está disponível no próprio sítio da AIEA em: https://www.iaea.org/newscenter/focus/dprk/chronology-of-key-events.

mísseis, mostrando uma evolução contínua (SETH, 2020, pp. 467-480; TERRY, 2021; NORTH Korea's Nuclear [...], s.d.).

Nye Jr., ao escrever sobre o futuro do poder e o poder cibernético, ao analisar o poder militar avalia o papel político das armas nucleares. Como seria esperado, as armas nucleares, apesar de diversos problemas, ainda exercem um papel importante na dissuasão. Tanto é verdade que estados menores continuaram a busca por este tipo de arma, como Irã e Coreia do Norte. A razão é que tais armas serviriam para deterem os EUA (no caso do Irã, Israel também), aumentar a influência regional e prestígio global. Assim, ele conclui que o tabu quanto ao uso de tais armas em guerras continua, mas ainda são peças importantes dentro da política internacional (NYE Jr., 2011, p. 54).

As armas nucleares da Coreia do Norte são consideradas a principal ameaça ao estado sul-coreano (KIM, LEE, 2023, p. 550). Entretanto, além delas, investigações sugerem que o país tem (ou ao menos pesquisou) outros tipos de ADM. Existe a possibilidade de a Coreia do Norte possuir um estoque entre 2500 e 5000 toneladas de agentes químicos de guerra. Como o país não assinou a Convenção de Armas Químicas (em inglês *Chemical Weapons Convention*, CWC) e, por consequência, não é fiscalizado pela Organização pela Proibição de Armas Químicas (OPAQ ou, em inglês, *Organization for the Prohibition of Chemical Weapons*, OPCW) (KASZETA, 2021, pp. 312-313), trata-se de uma suspeita. O histórico de posse ou produção desse tipo de ADM vem desde a Guerra da Coreia e de colaborações com a União Soviética desde a década de 1960. Recentemente, há informações de colaboração entre a DPRK e com a Síria na colocação de ogivas químicas (contendo sarin e gás VX) em mísseis SCUD-D[129], os quais são utilizados por ambos os países. Em fevereiro de 2017, Kim Jong-nam, meio-irmão de Kim Jong-um, foi assassinado no aeroporto de Kuala Lumpur, Malásia, com o uso de VX, sendo mais um indício da existência desse tipo de ADM no país (KASZETA, 2021, pp. 231-234). Com relação a armas biológicas, o país é signatário da Convenção para a Proibição de Armas Biológicas e Toxínicas (em inglês *Biological and Toxins Weapons Convention*, BWC), entretanto não tem mantido o compromisso assumido (DIA, 2021, p. 28). Segundo relatório de 2024 da inteligência estadunidense, o país mantém capacidade de uso militar tanto de armas biológicas quanto químicas (DNI, 2024, p. 21; KASZETA, 2021, pp. 312-313). Por fim, outros países aparentemente não têm implementado políticas preventivas contra a exportação de material de uso dual para a Coreia do Norte (KIM *et al.*, 2017, p. 24).

[129] Os SCUD-D são mísseis balísticos de curto alcance (SRBM, do inglês *Short-range Ballistic Missile*), os quais possuem alcance entre 300 e 1000 m. São aprimoramentos a partir dos mísseis SCUD originais da União Soviética, correspondendo à sua quarta geração (MISSILE DEFENSE PROJECT, 2024).

O relatório de 2009 sobre armas químicas e biológicas da Coreia do Norte, elaborado pelo *International Crisis Group*, afirma o seguinte:

> Numerosas instituições internacionais especializam-se no desarmamento e na criação de confiança no que diz respeito às armas de destruição em massa. Contudo, a Ásia Oriental não compartilha da experiência da Europa em matéria de instituições multilaterais fortes, especialmente no domínio da segurança. Alguns mecanismos são universais e indispensáveis, como o Tratado de Não Proliferação Nuclear (TNP), a Agência Internacional de Energia Atômica (AIEA) e a CWC, mas até agora têm sido insuficientes para lidar com as ADM norte-coreanas. Isto levou à proliferação de instrumentos *ad-hoc* nas últimas duas décadas: o *Agreed Framework*, o *Four-Party Talks*; o *Six-Party Talks*; cúpulas intercoreanas; reuniões ministeriais intercoreanas; conversações militares intercoreanas; e *Track II Dialogues*. Nenhum mecanismo único pode resolver todas as questões pendentes em torno das ADM norte-coreanas e da segurança regional, pelo que será necessária uma colcha de retalhos de questões existentes e novas para que a diplomacia tenha sucesso[130] (INTERNATIONAL CRISIS GROUP, 2009, p. 18, tradução minha).

Percebe-se que se mantiveram, em paralelo, diversas mesas de diálogo abertas, sempre com a participação das duas Coreias e outros interlocutores, sobre a existência de ADM na Coreia do Norte. O fato é que o país alcançou bons resultados nas armas nucleares e seus métodos de entrega (foguetes). Primeiramente com o apoio externo, adquirindo conhecimento para, atualmente, executar a construção, desenvolvimento e pesquisa de forma nativa, através de seu próprio pessoal. É razoável imaginar que outros países, que não sejam as grandes ou médias potências, poderiam, também, alcançar o mesmo objetivo (MILLER, NARANG, 2017).

Seguindo o ex-diretor da CIA, James Woolsey, em 1993, os EUA viviam até pouco tempo antes em um mundo bipolar, onde se percebia como única grande ameaça um dragão (no caso, a União Soviética). Após derrotarem-no, eles estariam sob múltiplas ameaças, como se passassem a se proteger ao mesmo tempo de diferentes cobras venenosas em uma floresta (KILCULLEN, 2020, p. 10-11). Na interpretação dele, a Coreia do Norte era uma dessas cobras. Sendo um estado fraco, depois de perder o apoio da União Soviética, com a Rússia ainda por se reerguer, e com a China ainda sem destaque, o país buscou formas de se proteger no novo ambiente por meio do armamento nuclear. Com isso, acabou virando um pequeno dragão, na interpretação de Kilcullen (2020, pp. 18, 31-36), contra o qual, agora, o país teria que contrapor.

---

[130] Texto original: "Numerous international institutions specialise in disarmament and confidence building with respect to weapons of mass destruction. However, East Asia does not share Europe's experience of strong multilateral institutions, particularly in the security realm. Some mechanisms are universal and indispensable, such as the Nuclear Non-Proliferation Treaty (NPT), the International Atomic Energy Agency (IAEA) and the CWC, but so far they have been insufficient for dealing with North Korean WMD. This has led to the proliferation of ad hoc instruments over the last two decades: the Agreed Framework; the Four-Party Talks; the Six-Party Talks; inter-Korean summits; inter-Korean ministerial meetings; inter-Korean military talks; and Track II dialogues. No single mechanism can resolve all outstanding issues surrounding North Korean WMD and regional security, so a patchwork of existing and new ones will be necessary if diplomacy is to succeed."

4.5 Sanções impostas à Coreia do Norte

Sanções são ações adotadas por países e agências, de modo uni ou multilateral, contra países ou agentes não-estatais a fim de puni-los ou influenciar suas atividades. Normalmente de natureza econômica, elas podem implicar consequências diplomáticas ou militares. No âmbito da ONU, compete a seu Conselho de Segurança a determinação de medidas como sanções, as quais devem ser seguidas por todos os países que compõem a organização. Conforme o artigo 41 do Capítulo VII ("Ação relativa a ameaças à paz, ruptura da paz e atos de agressão") da Carta das Nações Unidas,

> o Conselho de Segurança decidirá sobre as medidas que, sem envolver o emprego de forças armadas, deverão ser tomadas para tornar efetivas suas decisões e poderá convidar os membros das Nações Unidas a aplicarem tais medidas. Estas poderão incluir a interrupção completa ou parcial das relações econômicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radiofônicos, ou de outra qualquer espécie e o rompimento das relações diplomáticas. (ONU, 1945, n.p.)

Após os mísseis lançados pela Coreia do Norte sobre o Japão em julho de 2006, a ONU emitiu a Resolução 1695 condenando tais lançamentos e exigindo que todas as atividades relacionadas ao seu programa de mísseis balísticos fossem suspensas (ONU, 2006a).

Em 14 de outubro de 2006, sete dias depois do primeiro teste nuclear pela Coreia do Norte, o Conselho de Segurança da ONU emitiu a Resolução 1718 devido ao programa de armas de destruição em massa, especialmente no que se refere ao desenvolvimento de armas nucleares (ONU, 2006b; SECURITY COUNCIL REPORT, 2015). A origem de tais sanções está relacionada ao impasse ou não cumprimento de diversas negociações ocorridas anos antes e à saída do TNP, conforme relatado na seção anterior. A mesma Resolução 1718 criou um comitê com a missão de cumprir tarefas referentes às sanções[131] (ONU, 2006b).

Em 12 de junho de 2009, o Conselho de Segurança emitiu a Resolução 1874, que criava um "Painel de Peritos"[132], nomeados com duração de um ano, sendo prorrogado ano a ano. Esse painel tinha por atribuição auxiliar o comitê anteriormente criado e fornecer subsídios quanto ao cumprimento ou não das sanções, propondo alterações, caso houvesse necessidade (ONU, 2009). Interessante reparar que, só a partir de 2018, os relatórios passaram a citar atividades relacionadas às capacidades cibernéticas do país e a sugerir alterações nas sanções para atender a estas questões.

---

[131] A lista complete e atualizada dos produtos e serviços sancionados, bem como os documentos referentes a este comitê está disponível em: https://www.un.org/securitycouncil/sanctions/1718. Acesso em: 25 jun. 2024.

[132] O termo original utilizado na resolução em inglês é *Panel of Experts*. "Painel de Peritos" é a tradução utilizada nos Decretos que internalizaram as Resoluções na legislação brasileira.

Em 28 de março de 2024, a Rússia, país com poder de veto no Conselho de Segurança da ONU, vetou a prorrogação do Painel de Peritos encerrando, assim, a emissão dos relatórios que subsidiam (ou deveriam subsidiar) o Comitê e as decisões do Conselho acerca dos temas que envolvam a Coreia do Norte e a aplicação das sanções a ela impostas (ARNOLD, 2024). A lista de indivíduos e entidades sancionados pela ONU, incluindo aqueles relacionados à resolução 1718, é de domínio público, e está disponível sempre atualizada no sítio da organização[133].

Aqui cabe uma observação: uma das atividades do Painel de Peritos era a fiscalização da implantação das resoluções do Conselho de Segurança em que constavam as sanções. Cada Estado-Membro é responsável por encaminhar, depois da emissão da resolução e num prazo determinado, um "relatório de implementação nacional", no qual consta como se encontra a implementação da resolução no país. O Painel contabilizava os relatórios recebidos e informava isso no relatório seguinte. A lista de Estados-Membros e seus relatórios, atualizada até 13 de setembro de 2024, está acessível no sítio da Internet da ONU[134]. No parágrafo 217 do último relatório emitido (S/2024/215 de 7 de março de 2024) lê-se:

> O painel observa que apenas 130 dos 193 estados membros encaminharam pelo menos um relatório de implementação nacional até dezembro de 2023. Isso significa que quase um terço de todos os Estados-Membros nunca enviou um relatório de implementação nacional ao Conselho de Segurança e, portanto, não estão atingindo sua obrigações quanto às resoluções[135] (ONU, 2024a, p. 69, tradução minha).

O que se depreende dessa informação é que os Estados-Membros podem não estar implementando as resoluções determinadas, em desconformidade com o artigo 41 do Capítulo VII da Carta da ONU (ONU, 1945), prejudicando a efetividade das sanções impostas à Coreia do Norte.

Destaco ainda que, em verdade, a última atualização das sanções ocorreu em 2017 com as resoluções S/RES/2356 (2017), S/RES/2371 (2017), S/RES/2375 (2017) e S/RES/2397 (2017) do Conselho de Segurança (ONU, s.d.). Desde então, a lista de sanções não foi atualizada e, portanto, pode não conter indivíduos ou organizações envolvidas com as novas capacidades cibernéticas desenvolvidas e relatadas pelo painel.

---

[133] Disponível em: https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list. Acesso em: 15 jan. 2025.

[134] Acessível em: https://main.un.org/securitycouncil/en/sanctions/1718/implementation-reports.

[135] Texto origina: "The Panel notes that only 130 of 193 Member States had submitted at least one national implementation report by December 2023. This means that nearly one third of all Member States have never submitted a national implementation report to the Security Council and are therefore not meeting their resolution obligations."

Para a Rússia, a Coreia do Norte também tem sido um parceiro estratégico enquanto fornecedor de equipamentos militares e munição, usados no *front* da Guerra contra a Ucrânia, iniciada em 2022. Esse apoio vem de algum tempo, com o fornecimento de armas convencionais desde este ano para o Grupo Wagner (MADHANI, LEDERER, 2022) e ao exército russo em 2023 (BAKER, 2023) e 2024 (SEO, REGAN, 2024; JAKEX, 2024; KIM, 2024). Recentemente os dois países assinaram um Tratado Abrangente de Parceria Estratégica (do original em inglês, *Treaty on Comprehensive Strategic Partnership*), apontando para um alinhamento estratégico entre eles e aprofundando suas relações. Kim Jong-un afirmou que dava apoio incondicional às políticas russas, e Vladimir Putin garantiu que seu país não se furtaria de uma cooperação técnico-militar com a Coreia do Norte (CHA, KIM, 2024). Ainda, desde o mês de outubro de 2024 foram enviadas tropas norte-coreanas para o front da guerra entre Rússia e Ucrânia (TERTITSKIY, 2024; CANCIAN, PARK, 2024). Tais ações listadas e o tratado violam diversas sanções da ONU, algumas das quais contaram com o voto favorável da Rússia no Conselho de Segurança. Contudo isso não tem sido uma restrição para os negócios entre os países (CRS, 2024). Com relação àquelas tropas norte-coreanas enviadas para a guerra, sabe-se que o acesso à Internet não é irrestrito na Rússia, mas é mais liberado que na Coreia do Norte. Isso tem feito com que tais militares acessem uma maior quantidade de sítios sobre assuntos mais diversos do que em seu país, como pornografia (HAGAN, 2024). Capturas recentes de soldados norte-coreanos permitiram a obtenção de um equipamento tipo *tablet* com informações do que é apresentado aos soldados que será analisado pelos serviços de inteligência da Ucrânia e Coreia do Sul (HARDING, 2025).

Desde a década de 1990 houve compras de armamento norte-coreano por outras nações parceiras, como Irã e Síria, bem como negociações dos mesmos itens (incluindo mísseis balísticos e tecnologia associada) já foram feitas por Egito, Iraque, Líbia, Paquistão, Iêmen e Myanmar. Burma, outro parceiro de outrora, aparentemente, tem se distanciado do país (DIA, 2021, p. 67; KIMBAL, 2008; TERRY, 2021; BERMUDEZ, Jr., 1999).

Os Estados Unidos da América mantém uma extensa lista de sanções contra a Coreia do Norte, que vão além daquelas do Conselho das Nações Unidas. O *Office of Foreign Assets Control* (OFAC), que fica dentro do Departamento do Tesouro dos EUA, mantém uma lista das sanções, incluindo orientações para o caso de suspeitas[136]. As sanções específicas contra o país seguidas são, atualmente, regulamentadas a partir da Ordem Executiva (EO) 13466, emitida pelo presidente George W. Bush, em conjunto com a Proclamação 8271, ambas em 26 de junho

[136] A lista de sanções pode ser acessada em: https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions.

de 2008. Outras EO seguiram-se a essa, acrescentando restrições. Chama a atenção a EO 13687 de 2 de janeiro de 2015, pelo presidente Barack Obama, a qual cita, dentre outras razões, referências ao ataque executado contra a Sony Pictures Entertainment no final do ano anterior. Outra ordem executiva do mesmo presidente, a EO 13722 de 15 de março de 2016, sanciona quem se envolver em atividades que minem a segurança cibernética contra alvos fora da Coreia do Norte, executadas em nome desta ou do Partido dos Trabalhadores Coreanos (CLAUSSEN, 2020, p. 349).

Quanto à China, outro país com assento permanente no Conselho de Segurança da ONU, esta mantém (na verdade tem incrementado) investimentos na Coreia do Norte para aproveitar sua mão de obra barata (PACHECO-PARDO, 2013, p. 98; NORTH Korea's Secrtet [...], 2018).

Um país de destaque na exportação de tecnologias cibernéticas é Israel, onde é desenvolvido o Pegasus[137], por exemplo. Este é um dos sistemas abarcados pela citada lei, prevenindo que sejam licenceados e usados pela Coreia do Norte. De acordo com o *Defense Export Control Act*[138], produtos relacionados à defesa, como o citado, não podem ser exportados para países sancionados pela ONU (RICHARD, RIGAUD, 2023, pp. 192-193). Claro que a cooperação existente entre a DPRK e Irã ou Síria indicam que esse tipo de proposta nem deve ser colocada à mesa.

O Conselho Europeu e Conselho da União Europeia, desde 2016, adotaram sanções adicionais àquelas determinadas pelo Conselho de Segurança da ONU. Elas incluem restrições de viagens para indivíduos, além de congelamento de ativos, restrição de disponibilização de fundos ou recursos econômicos a indivíduos e entidades, bem como outras restrições diversas quanto a comércio, bens e tecnologia que possam auxiliar o desenvolvimento de ADM[139].

No entendimento do Brasil, somente o Conselho de Segurança da ONU tem a atribuição de impôr sanções a países, sendo que tem adotado e cumprido as que foram por ele determinadas (MARCONDES, 2022, p. 13).

4.6 Relações com o Brasil

Quanto às relações históricas recentes com o Brasil, há alguns fatos interessantes. O Brasil recebeu insistentes pedidos do presidente estadunidense Harry Truman para enviar tropas

[137] O Pegasus é um *spyware* para celulares, desenvolvido pela empresa israelense NSO Group Technologies Ltd., considerado o estado-da-arte, com grande poder ofensivo, de difícil detecção (RICHARD, RIGAUD, 2023, p. 6).
[138] Tradução livre: Lei de Controle de Exportação de Produtos de Defesa.
[139] Disponível em: https://www.consilium.europa.eu/pt/policies/sanctions-against-north-korea/. Acesso em: 21 jan. 2025.

ao teatro de operações da Guerra da Coreia. Entretanto, todos foram negados, não sem muita discussão na alta cúpula militar, além da proposta também não contar com o apoio do presidente Getúlio Vargas nem da esquerda (DAVIS, 2002; RICUPERO, 2017, p. 383). Já após a separação da península entre dois países, a Coreia do Norte, apoiando forças de esquerda, teria, entre os anos de 1968 e 1971, enviado US$ 50 mil e treinado componentes dos grupos Ação Libertadora Nacional (ALN) e Vanguarda Popular Revolucionária (VPR), que lutavam contra a ditadura brasileira, além de auxiliado a estruturar um campo de treinamento, possivelmente em Porto Alegre (BERMUDEZ, Jr., 1990, pp. 64-65; GODOY, 2009; ALN ganhou [...], 2009). Para ilustrar a relativa proximidade do país com os militantes contra a ditadura, nove componentes do VPR viajaram para treinamento no país asiático por três meses (GODOY, 2009; GODOY, 2014, p. 102). Darci Toshiko Miyaki, em entrevista para o Memorial da Resistência de São Paulo, afirma ter sido a primeira brasileira a viajar para a Coreia do Norte, onde executou tarefas pela ALN. Ela viajou a partir de Cuba, país onde se exilou quando passou a ser procurada pela ditadura brasileira (MIYAKI, 2014; MEMORIAL DA RESISTÊNCIA, s.d.; PEREIRA, 2015). Um fato simbólico que representa essa aproximação foi que a ALN deu um relógio da marca Rolex ao Marechal Kim Il-sung, obtido em um assalto executado pelo grupo a uma joalheria (BARBO, 2023; ALN ganhou [...], 2009).

Além disso, na década de 1990, com o fim da ditadura, houve a emissão de passaportes brasileiros pela embaixada brasileira em Praga, na República Tcheca, para o líder supremo Kim Jong Il e seu filho Kim Jong Un, utilizando nomes falsos. Os documentos teriam sido emitidos em 26 de fevereiro de 1996 e usados em viagens e para solicitar vistos para países ocidentais (FALCONBRIDGE, 2018). Já se levantou a possibilidade de uso dos passaportes para preparação de possível fuga da Coreia do Norte, se necessário (KIM JONG-IL'S [...], 2018), mas não se conseguiu confirmação disso por fontes abertas. A emissão dos passaportes teria sido feita sob a coordenação do já citado *Bureau 39* (KIM JONG-IL'S [...], 2018). O Ministério das Relações Exteriores do Brasil não emitiu comunicados oficiais esclarecendo o assunto.

Por fim, outro caso interessante é o do time de futebol Clube Atlético Sorocaba, que jogou em Pyongyang um jogo amistoso em 5 de novembro 2009 contra o selecionado nacional daquele país. O time paulista fora apresentado ao público como se tratasse da seleção brasileira de futebol. O convite para o jogo ocorreu devido ao fato de ele ser propriedade da Igreja da Unificação de Sun Myung Moon. Reverendo Moon, como é mais conhecido, nasceu numa cidade onde hoje é a Coreia do Norte e ficou preso em campos de trabalho durante a Guerra da Coreia, sendo libertado pelo exército da ONU, indo morar na Coreia do Sul. Apesar de se posicionar contra o marxismo, manteve-se com conexões com Kim Il-sung, o que explica tal

convite. O relacionamento do religioso com o Brasil, entretanto, vem desde antes, quando comprou terras em Mato Grosso do Sul, criando uma comunidade com imigrantes sul-coreanos. O time de futebol veio depois, já que ele buscava investimentos e entendia que o esporte seria uma forma de “cura para o ódio humano”. (LANG, 2024, n.p.; RÁDIO NOVELO [...], 2023, n.p.).

Os países formalizaram relações diplomáticas em 9 de março de 2001, durante o governo Fernando Henrique Cardoso, com a embaixada da DPRK em Brasília sendo inaugurada somente em janeiro de 2005, já no governo Luís Inácio Lula da Silva. O Brasil, por sua vez, anunciou sua embaixada em Pyongyang em setembro de 2008, recebendo o primeiro embaixador em 2009. Um dos motivos do atraso do Brasil no envio do diplomata foram os testes nucleares que ocorreram em maio de 2009, aos quais o Brasil se opôs. Ainda que as relações bilaterais sejam cordiais, questões como os direitos humanos são caras à diplomacia brasileira, com o país apoiando várias ações da ONU ligadas ao tema, inclusive diretamente relacionadas com a Coreia do Norte. Ainda, sempre que ocupou um assento rotativo no Conselho de Segurança da ONU, o Brasil votou a favor de sanções e se posicionou contra a nuclearização da Coreia do Norte, condenando seus testes nucleares e sugerindo o retorno do país ao Tratado de Não-Proliferação Nuclear (TNP) (MARCONDES, 2022; SIEBRA, 2017).

5 A COREIA DO NORTE NO ESPAÇO CIBERNÉTICO

Neste capítulo, mostro como a Coreia do Norte se estruturou e se apresenta no espaço cibernético, além de mostrar, em seguida, suas capacidades cibernéticas e avalições destas feitas por estudos acadêmicos e de empresas. Também ilustro alguns usos ofensivos dados para tais capacidades, levanto as possíveis formas de cooperação que o país pode estar envolvido e avalio como seriam as ações ofensivas executadas por outros contra sua estrutura cibernética.

A Coreia do Norte está longe de ser reconhecida pela sua estrutura de telecomunicações e conectividade à Internet. O tamanho desta rede dentro do país foi determinado de uma forma curiosa: no dia 19 de setembro de 2016, uma configuração errada de um dos servidores-raiz de DNS do ccTLD .kp, correspondente ao país norte-coreano[140], permitiu que qualquer máquina conectada à Internet acessasse todo o mapa de DNS do servidor. Esse vazamento permitiu verificar que, naquela época, só haveria 28 sítios de Internet no país (FRANCESCHI-BICCHIERAI, 2016B)[141], confirmando o tamanho diminuto da sua estrutura da Internet[142]. Um estudo da empresa Trend Micro, de 2017, levantou os endereços IPv4 designados ao país, os quais consistiam em algumas faixas classe C de endereços e outros conjuntos menores. No total, seriam pouco mais de 10 mil endereços IPv4 (KROPOTOV *et al.*, 2017). Recorded Future (2017, pp. 19-20) em seu levantamento, por sua vez, já relata somente 1.536 endereços. Sobre usuários, os dados são incertos, já que não há informações oficiais nem pesquisas de campo no país sobre o tema. Foram estimados em 20 mil, em julho de 2022, o que corresponde a 0,1% da população norte-coreana (IWS, 2024).

A dimensão reduzida da rede e do seu alcance não impediu o desenvolvimento de suas capacidades cibernéticas, muito devido a colaborações com países vizinhos. O desertor norte-coreano Kim Heung Kwang disse, em uma entrevista, que auxiliou no treinamento dos primeiros espiões da Coreia do Norte que utilizaram o espaço cibernético. Segundo ele, em 1992, experts norte-coreanos em computação retornaram da China afirmando que os chineses utilizariam a Internet para furtar segredos e atacar inimigos do governo, e que a Coreia do Norte deveria fazer o mesmo. Segundo o mesmo desertor, a capacitação teria sido iniciada em 1996, e em 1998 o *Bureau 121* foi formado. Nesse intervalo, o trabalho era observar e aprender sobre

[140] Atribuído em reunião dos diretores da ICANN em 24 de setembro de 2007. A título de comparação, o ccTLD do Brasil (.br) foi atribuído em 18 de abril de 1989.
[141] O vazamento de dados está disponível no GitHub, plataforma de compartilhamento e colaboração de projetos de desenvolvimento, hoje pertencente à Microsoft, na URL: https://github.com/mandatoryprogrammer/NorthKoreaDNSLeak. Acesso em: 6 mar. de 2024.
[142] Para comparação, o Brasil possui 5.374.242 domínios registrados, conforme dados do Registro.br disponível em: https://registro.br/dominio/estatisticas/. Acesso em: 20 jan. 2025.

a Internet dos países alvo, e não atacar. Tempos depois, o recrutamento, que antes abrangia o pessoal militar, passou a ser realizado diretamente nas escolas secundárias, selecionando os estudantes com maior aptidão em matemática para as suas melhores universidades, alguns dos quais poderiam ser selecionados para as melhores do país, como a Universidade Militar Kim Il-sung[143] (tida como a melhor) ou Universidade de Tecnologia Kim Chaek. A Universidade Kim Il-sung estaria formando, em 2009, por volta de cem novos operadores para executar ataques. Na mesma época, cidadãos designados para trabalhos na ONU matriculavam-se em cursos de computação em universidades de Nova Iorque (SANGER, 2018, pp. 127-129; BUCHANAN, 2020, p. 269-270; YOON, 2011; WHITE, 2020, pp. 68-69; WHITE, 2022; EUA, 2020, p. 9-16; MCWILLIAMS, 2003). Até esse ponto, percebe-se que não há nenhuma ilegalidade, ainda, dentro das ações do governo norte-coreano que, a seus olhos, buscava capacitar sua população em uma tecnologia cuja presença aumentava, bem como em suas aplicações como, por exemplo, o comércio eletrônico.

Dentro do país, nos anos 2000, e-mails só podiam ser enviados de uma instalação em Pyongyang por meio de uma conexão com a cidade chinesa de Shenyang[144] que era, de tempos em tempos, acionada. Somente em 2006 a conexão passou a ser permanente (ou dedicada, no jargão técnico), ainda voltada a e-mails e outros poucos serviços. O primeiro serviço de banda larga foi instalado em Pyongyang, também restrito. Em 2016, Internet para alunos de universidades era limitada a estudantes de pós-graduação, e os cidadãos comuns não tinham acesso a ela, somente a uma *intranet* estatal, de nome Kwangmyong (광명, traduzido como "luz"). Tal rede oferece serviços básicos de informação, e-mail e rede social, por exemplo, conectando bibliotecas, universidades e governo (WILLIAMS, 2016; CARLIN, 2018, pp. 317-318).

Com relação à conectividade à Internet, um relatório da Hewlett Packard Security Research de 2014 mostra que, ao menos à época, haveria uma colaboração entre chineses e norte-coreanos, tanto na conectividade, por meio da China Unicom, quanto no fornecimento dos equipamentos computacionais e de comunicação necessários, como servidores e roteadores O acesso físico local, feito por meio de fibras ópticas, é oferecido desde 2010 pela Star Joint Venture (Star JV), uma *joint venture* entre o governo e a empresa tailandesa Loxley Pacific Co., conectando o país, então, à Internet por meio da China Unicom (HP, 2014, pp. 10-11, 42). Em 2015, os tailandeses retiraram seus investimentos na Star JV, e em 2018 cessaram todos os

[143] Anteriormente chamada de Universidade Mirim (*Mirim College* nos artigos em inglês) (JUN *et al.*, 2015, p. 42).
[144] Esta cidade está a 3 horas de carro da fronteira entre os países.

investimentos que tinham no país (ONU, 2009a, p. 329). Até 1º de outubro de 2017 este se tratava do único ponto de conexão, quando a empresa russa TransTeleCom (TTK) passou a também prover conectividade à Internet para a Coreia do Norte. No país há redes celulares 3G, viabilizadas pela empresa Korea Posts and Telecommunications (KPTC, nome fantasia: Koryolink), a qual é uma *joint venture* entre o governo e a companhia egípcia Orascom Telecom Media & Technology Holding (WILLIAMS, 2016; CCC, 2014; NEWTON, PARK, 2017). Em 2024 a estatal Kangsong[145] também passou a oferecer acesso 4G (WILLIAMS, 2024a).

Segundo relatado por Scott, em 2014, a rede da universidade onde lecionava dava acesso não à Internet, mas a uma *intranet* que serve só páginas do próprio país, sem um ponto de conexão (*gateway*) entre essa rede e a Internet.[146] Também segundo Scott, aos estrangeiros não seria dado acesso à *intranet*, mas sim à Internet. Além disso, esse acesso à Internet seria feito por meio de um servidor *proxy*[147] com autenticação (CCC, 2014). Uma análise do tráfego de Internet originário da Coreia do Norte realizado pela Recorded Future em 2017, mostrou que os usuários com permissão de acesso à rede mundial navegam por serviços de forma bastante similar aos usuários de outros países: acessam serviços, conteúdo de cultura, notícias, vídeos, mídias sociais e sítios de compra. Importante destacar que esse tráfego é gerado pelos usuários que têm permissão de acesso à Internet (0,1% dos cidadãos do país) (RECORDED FUTURE, 2017).

Quanto ao ensino, há relatos do ensino de ciência da computação desde a década de 1980, inclusive com o envio de alunos norte-coreanos para a Alemanha Oriental. Segundo relatado, computadores existentes no país, nessa época, seriam originários da Europa, especialmente Polônia, Japão e Singapura (MARTIN, 2004). No documentário *The Propaganda Game*, de 2015, ao filmar o laboratório de computação de uma universidade, a equipe observa computadores de marcas conhecidas no Ocidente e pergunta ao guia que os acompanhava onde adquiriam tais equipamentos. O guia se negou a responder afirmando que, se falasse, eles tentariam barrar tais aquisições (PROPAGANDA [...], 2015). Atualmente, universidades de tecnologia no país chegam a ter professores visitantes de países que não são

[145] Propriedade do Ministério da Indústria da Informação da Coreia do Norte (WILLIAMS, 2024a).

[146] Outros países já têm ou tiveram estruturas semelhantes nas quais os usuários ficam restritos a uma rede interna ao país e, ao acessarem algo externo, podem sofrer algum tipo de filtro ou fiscalização. China, Rússia, Irã, Síria e Burma são exemplos (CLARKE, KNAKE, 2019, p. 208).

[147] Simplificadamente, o serviço de *proxy* funciona da seguinte forma na Web: o navegador solicita ao servidor *proxy* o arquivo que gostaria de acessar, como uma página Web, imagem, arquivo de som, vídeo... O servidor então repassa a requisição a outro servidor, onde o arquivo solicitado se encontra, e encaminha ao navegador solicitante. O fato de ele ser autenticado permite que, por exemplo, sejam configurados filtros sobre o que pode ser ou não acessado (por exemplo que servidores, tipos de conteúdo ou arquivos são bloqueados) conforme o perfil do usuário autenticado, além de que todo acesso que este fez fica registrado em arquivos de histórico (também chamados de *logs*).

aliados, com relatos bastante interessantes disponíveis, tais como os de Will Scott (CCC, 2014) e Suki Kim (KIM, 2014).

Dentre as tecnologias desenvolvidas na Coreia do Norte, a que pode trazer mais curiosidade é o RedStar OS, um sistema operacional nacional baseado no sistema operacional de código aberto Linux[148] (GREENBERG, 2022; SELIGER, SCHMIDT, 2014, pp. 74-75; CCC, 2014). Entretanto, não se trata de um sistema operacional encontrado nos computadores vendidos no país, em sua maioria de marcas chinesas e com Microsoft Windows XP ou Windows 7 instalado. Segundo relatado por Scott em sua apresentação, seria um sistema operacional normalmente encontrado em sistemas desenvolvidos pelo Korea Computer Center (KCC), principal unidade de pesquisa e desenvolvimento em TI do governo norte-coreano, fundada em 24 de outubro de 1990.

Outro centro de desenvolvimento é o Pyongyang Informatics Center (PIC), inaugurado em julho de 1986 (CCC, 2014; SELIGER, SCHMIDT, 2014, p. 74; BERMUDEZ, Jr., 2015, p. 240; Jun *et al.*, 2015, pp. 53-59). O KCC desenvolveu alguns produtos para o varejo também, como o navegador Naenara (내 나라, traduzido como "meu país"), baseado no Mozilla Firefox, que também dá nome a um sítio[149] e uma ferramenta de busca. Acessando-se o sítio pela Internet, são apresentadas páginas distintas daquelas acessadas por meio da intranet estatal (Kwangmyong). Outros produtos originários do KCC são o *tablet* Samjiyon, cujo sistema operacional tem o Android como base[150] (WILLIAMS, 2013), e o *tablet* Ullim, o qual conta com características de vigilância do usuário e restrição de acesso bastante inovadoras (WILLIAMS, 2017). Ambos os equipamentos eram produzidos na China. O PIC é menor que o KCC, sendo voltado ao desenvolvimento de *software* (JUN *et al.*, pp. 57-59).

5.1 Capacidades cibernéticas norte-coreanas

Inicialmente, cumpre esclarecer que a estratégia e doutrina militares da Coreia do Norte são teorizadas de fora do país por pesquisadores por meio de notícias domésticas e relatórios públicos das reuniões do KWP, além de eventuais documentos internos que vazam. Além disso, o país utiliza a desinformação como meio para propagar informações falsas ou imprecisas sobre suas capacidades efetivas (JUN *et al.*, 2015, p. 2-3, 26). Dessa forma, algumas das diversas

[148] Telas do RedStar OS podem ser vistas em: http://www.instiz.net/pt/1521630.
[149] Sítio acessível pela Internet em: https://www.naenara.com.kp/.
[150] Avaliações do equipamento podem ser lidas em: http://www.38north.org/wp-content/uploads/2013/10/SamjiyonProductReview_RFrank102213-2.pdf e http://www.northkoreatech.org/2013/08/01/review-samjiyon-tablet/.

fontes utilizadas discordavam entre si, entretanto sem prejudicar a conclusão. Quando pertinentes, tais diferenças são destacadas ao longo do texto.

Em 2003 já se tinha notícia de técnicos norte-coreanos de empresas de TI sendo contratados para desenvolver diversos tipos de *software* para governos e empresas para vários países da Europa, além de Japão, Coreia do Sul, Índia e China (MCWILLIAMS, 2003; TJIA, 2011). Entretanto, até 2009 a Coreia do Norte não se tratava de um país valorizado pelas suas capacidades cibernéticas. A partir de então, e principalmente depois de 2011, quando Kim Jong-un sucedeu seu pai, essas capacidades foram sendo incrementadas, cumprindo o que disse que a capacidades de guerra cibernética seriam uma "espada de múltiplos propósitos" (SANGER *et al.*, 2017, n.p.; KONG *et al.*, 2019, p. 1; MCWILLIAMS, 2003, n.p.). O diretor do Serviço Nacional de Inteligência da Coreia do Sul, Nam Jae-joon, relatou ao Comitê de Inteligência da Assembleia Nacional sul-coreana, em novembro de 2013, a seguinte fala de Kim: "guerra cibernética é uma espada de múltiplos propósitos que garante às Forças Armadas do Povo Norte-coreano uma capacidade implacável, junto às armas nucleares e mísseis"[151] (KONG *et al.*, 2019, p. 1, tradução minha).

As capacidades cibernéticas do país constavam de poucos relatórios emitidos até o ano de 2013. Desde então, os efeitos das delas começaram a ficar mais evidentes. Num artigo jornalístico publicado em 2 de dezembro de 2014, Perlroth afirmava que a Coreia do Norte, na época, era muito citada como uma possível ameaça cibernética, não muito pela sua competência, mas pela motivação de causar destruição, numa preocupação semelhante ao Irã. À época, um relatório recém-lançado da empresa Cylance[152] citava o ataque à Sony Pictures como um destaque naquele ano e mencionava que as características do ataque se assemelhavam às de outros executados contra bancos sul-coreanos, os quais ainda não tinham sido atribuídos a algum grupo. (PERLROTH, 2014). O relatório de 2015 do *Center for Strategic & International Studies* (CSIS) sobre o país afirmou que diversos especialistas foram tomados de surpresa, quando o FBI e o governo do Estados Unidos oficialmente atribuíram, em 19 de dezembro de 2014, uma sequência de ataques, incluindo o chamado *Sony Pictures Hack*, àquele país (JUN *et al.*, 2015, p. iv). Até então, poucos ataques de sabotagem tinham sido atribuídos de forma oficial a grupos norte-coreanos (BUCHANAN, 2020, p. 169).

[151] Texto original: "Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles."

[152] A empresa foi comprada, em 2019, pela Blackberry Limited, cujo nome anterior era Research in Motion (RIM), conhecida pelos seus aparelhos celulares tipos *smartphones*. Em dezembro de 2024, a Cylance foi adquirida pela empresa de segurança cibernética Arctic Wolf.

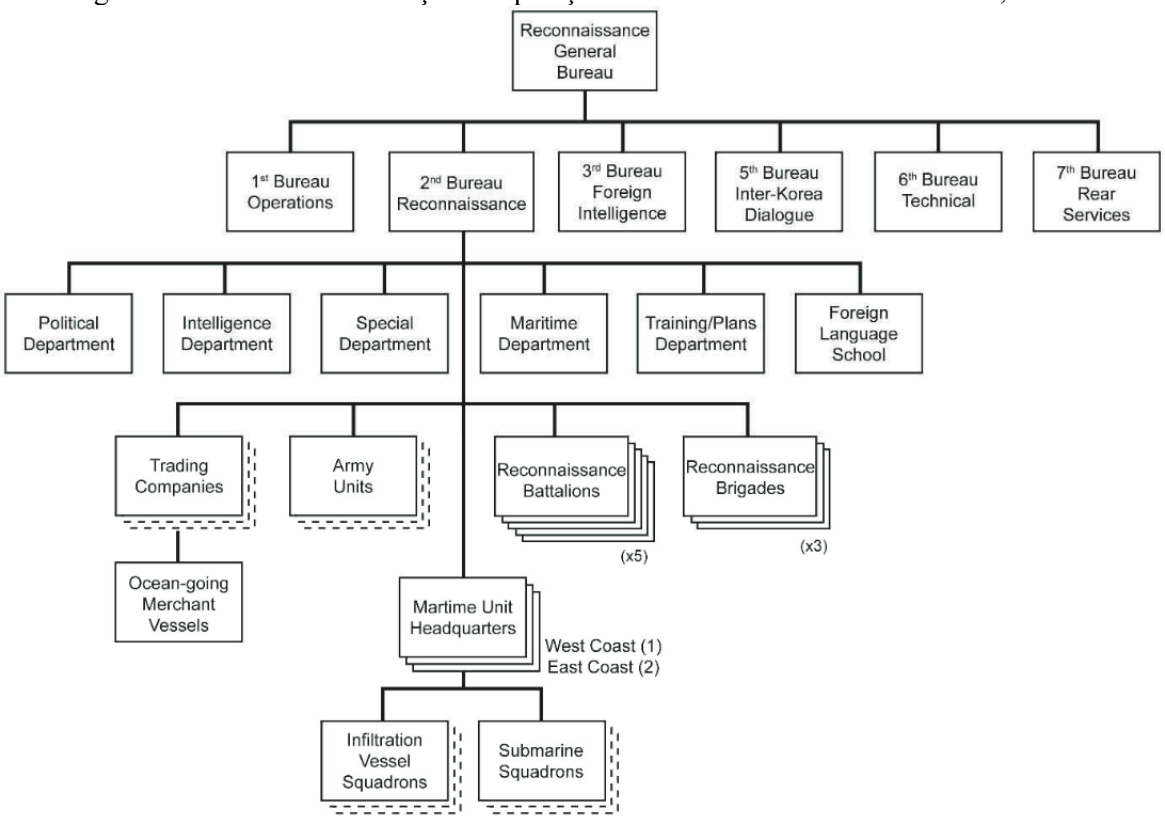
Já se afirmou que a Coreia do Norte seria um país dependente da China para suas capacidades cibernéticas (GARTZKE, LINDSAY, 2019, p. 220). Entretanto, há outros que reconheceram a evolução do país ao desenvolver suas capacidades para aplicá-las no espaço cibernético. O general de divisão do Exército da Coreia do Sul, In-bun Chun, foi claro ao dizer e repetir, para uma plateia de 1400 pessoas, num evento relacionado ao Exército Americano, em 2018, que "a Coreia do Norte é uma superpotência cibernética" (CLARK, 2018, n.p.). Izycki (2021, p. 59) não encontrou registros de compras de ferramentas cibernéticas ofensivas no mercado internacional – o que é esperado, considerando as sanções que lhes são impostas. Por isso, afirma que as ferramentas utilizadas seriam só aquelas desenvolvidas internamente. Perlroth (2021, p. 151) cita como o mercado de "*softwares* de comando e controle de intrusão"[153], nos Estados Unidos, é desregulamentado, exceto caso se enquadrem na lei de exportação de criptografia. Entretanto, a venda de tais sistemas permanece proibida a países embargados, como é o caso da Coreia do Norte.

Outra possibilidade de se obter tais ferramentas seria a aquisição no mercado clandestino, sendo que um deles está mais próximo do Brasil do que se pensa: na Argentina (PERLROTH, 2021, pp. 253-266). E a última é o furto, i.e., ataques cibernéticos contra outros grupos para obtenção do seu ferramental. Como exemplo de furto tem-se o caso do grupo Shadow Brokers contra a NSA, já citado neste trabalho, cujas ferramentas foram disponibilizadas posteriormente na Internet.

Entre 2009 e 2010 houve a revisão da Constituição do país (de 1998) e, na mudança, foi feita uma reorganização significativa do Estado norte-coreano. As operações clandestinas da Coreia do Norte passaram a ser reunidas em um só órgão de inteligência, o *Reconnaissance General Bureau* (RGB)[154]. Esse órgão foi formado combinando o *Operations Bureau*, do KWP, e o *Reconnaissance Bureau*, do *Ministry of People's Armed Forces* (Ministério das Forças Armadas Populares, numa tradução livre). O novo órgão passou a contar com uma estrutura de seis departamentos (*Bureaus*) (BERMUDEZ Jr., 2010; CARLIN, 2018, p. 318; JUN *et al.*, 2015), conforme pode ser visto no organograma da Figura 7.

[153] Texto original: "Command and control intrusion software."
[154] Em alguns documentos pode ser encontrado com o nome de *Unit 586* ou *586th Army Unit* (Jun *et al.*, p. 3).

Figura 7 – Estrutura dos serviços de operações clandestinas da Coreia do Norte, 2010[155]

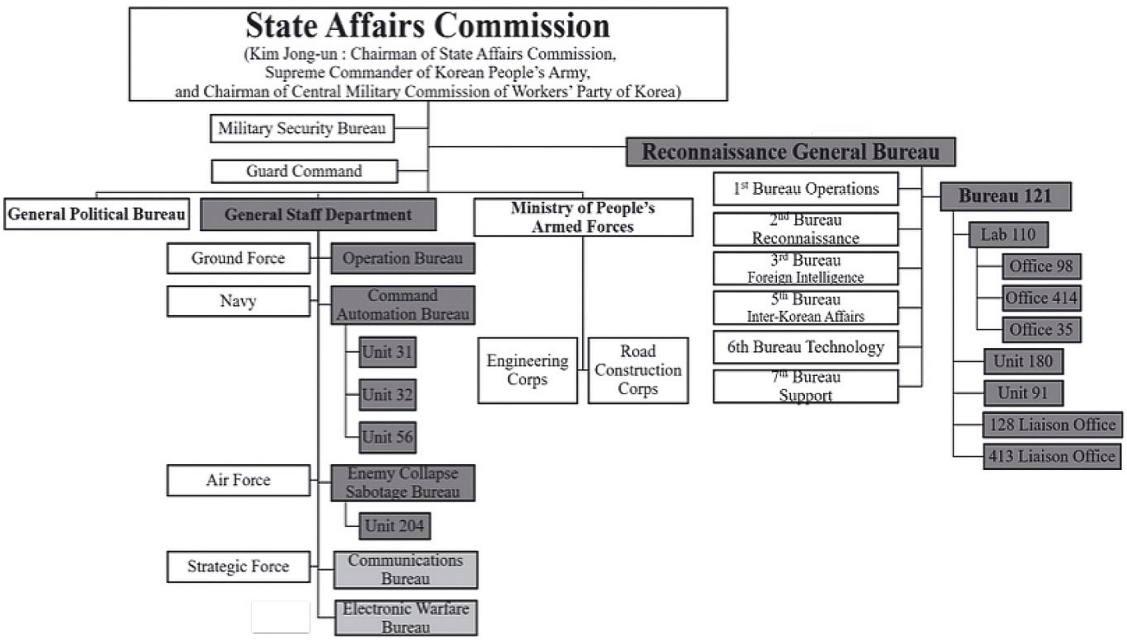


Fonte: Figura 5 de Bermudez Jr, (2010, p. 5).

Em 2013 foi incluído um sétimo *Bureau*, denominado *Bureau 121*, ao qual foram atribuídos o projeto e a execução de ataques cibernéticos (JUN *et al.*, 2015, p. 38). Um desertor da Coreia do Norte cita que este *Bureau* teria sido criado ainda em 1998 (SANGER, 2018, p. 128), entretanto, não cita qual sua posição no organograma, nem se seria um órgão do governo ou do partido. O levantamento feito por Kong *et al.* (2019), ilustrado na Figura 8, mostra como seria o possível organograma do RGB.

[155] A explicação de não haver um *4th Bureau* dentro da RGB é curiosa: para os coreanos, o número 4 está associado ao mau agouro, criando o que se chama de tetrafobia, porque a sua pronúncia em coreano (bem como no chinês) é similar à da palavra "morte" (OSBORNE, 2023).

Figura 8 – Estrutura dos serviços de operações clandestinas da Coreia do Norte, 2019



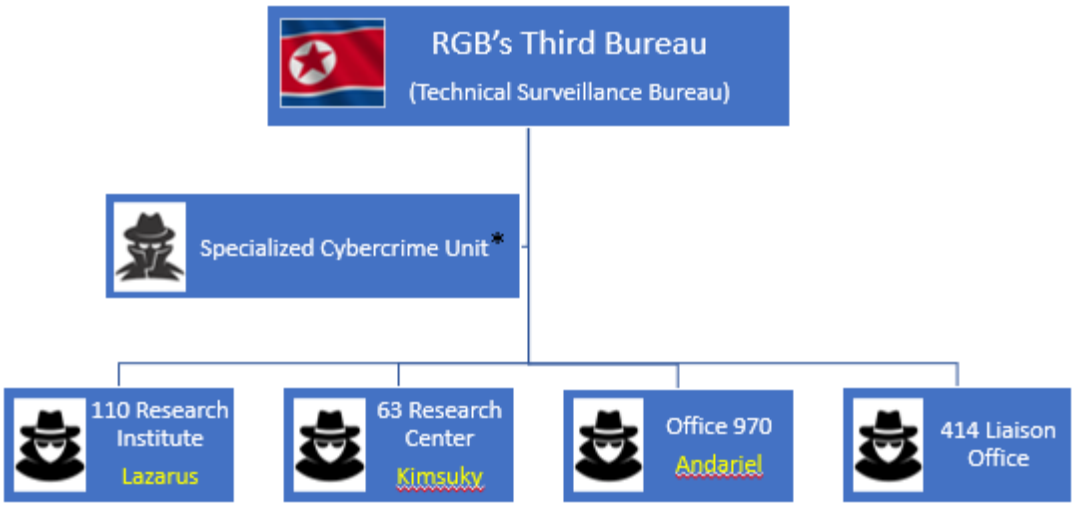
Fonte: Kong *et al.* (2019, p. 4).

Os autores do diagrama anterior afirmam que as unidades mais escuras na imagem são aquelas diretamente relevantes para operações cibernéticas, ao passo que as duas mais claras (de comunicações e guerra eletrônica) "têm potencial para conduzir capacidades cibernéticas" (KONG *et al.*, 2019, p. 4). As atribuições dessas duas unidades são mais voltadas ao que é chamado de *electronic warfare* (EW) e *electronic information warfare* (EIW) (Jun *et al.*, pp. 49-51; BERMUDEZ, 2005).

Estima-se que haja entre seis e sete mil operadores capacitados para a execução de ações cibernéticas ofensivas no *Bureau 121*, incluindo aqueles que operam a partir de outros países (RECORDED FUTURE, 2023, p. 3; EUA, 2020, p. E-1; KIM JONG-IL'S [...], 2018). Interessante relatar que outros nomes são usados em fontes abertas para este *Bureau*, como *Unit 121* e *Cyber Warfare Guidance Unit* (ou *Bureau*). O uso de nomenclaturas diferentes para as mesmas unidades e a mudança propositada do organograma em documentos externos faz parte dos esforços norte-coreanos de dificultar o entendimento da estrutura do Estado (JUN *et al.*, 2015, p. 40-41). Algumas fontes oficiais do governo dos EUA não reconhecem o *Bureau 121*, colocando as ações cibernéticas dentro do que seria o *6º Bureau* (tecnologia) (EUA, 2017, p. 14; DIA, 2021, pp. 57-58). O relatório S/2023/171 do Painel de Peritos da ONU, por sua vez, informa uma organização diferente para o RGB, com seis *bureaus* com as seguintes funções: "vigilância terra-ar (primeiro), análise informacional (segundo), vigilância técnica (terceiro),

inteligência externa (quinto), assuntos intercoreanos (sexto), apoio (sétimo)"[156] (ONU, 2023a, p. 69). O mesmo relatório coloca uma unidade especializada em crimes cibernéticos e grupos relacionados a ações cibernéticas subordinados ao terceiro bureau, citando como fonte Estados-membros da ONU, conforme ilustrado na Figura 9.

Figura 9 – Estrutura cibernética do terceiro *bureau* do RGB, segundo Painel de Peritos.



Fonte: ONU (2023, p. 69).

Essa estrutura, entretanto, não foi observada em outros relatórios, nem mesmo entre aqueles da própria ONU. O relatório S/2019/171 (ONU, 2019a, p. 49) cita um relatório do Congressional Research Service (CRS) dos EUA, de 2017, o qual aponta para o relatório da CSIS, de 2015 (CHANLETT-AVERY, 2017, p. 2). Este relatório, por sua vez, cita a organização da RGB como sendo a sugerida por JUN *et al.* (2015, p. 39), que apresenta uma estrutura bastante similar ao levantamento de Kong *et al.* (2019, p. 4), já apresentado na Figura 8.

Para executar os ataques, os grupos o fazem fora do território da Coreia do Norte, de modo a fugir da banda de rede limitada. Isso pode ser feito através de conexões remotas, com o operador fisicamente na DPRK, ou então com o operador no outro país. A Recorded Future (2017, pp. 24-25) exemplifica os seguintes países como bases para ataques: Índia, Malásia, Nova Zelândia, Nepal, Quênia, Moçambique, Indonésia e, com maior ênfase, China. Um relatório de 2020 do Exército dos EUA já dá como exemplos Belarus, China, Índia, Malásia e

[156] Texto original: "Land Air Surveillance (first), Information Analysis (second), Technical Surveillance (third), Foreign Intelligence (fifth), Inter-Korean affairs (sixth) and Support (seventh)."

Rússia (EUA, 2020, p. E-1). Como o RGB é o órgão responsável por operações clandestinas, uma das atividades é a de criar e manter empresas de fachada no exterior. Portanto, é razoável afirmar que são usadas como base para ataques por meio da Internet, contornando as limitações de sua ínfima estrutura, além de outras atividades como obtenção e lavagem de dinheiro (WHITE, 2020, p. 71; RECORDED FUTURE, 2017, pp. 24-25). As capacidades cibernéticas da Coreia do Norte e seu uso chamaram a atenção do Painel de Peritos criado pelo Conselho de Segurança da ONU. Tanto que, partir do ano de 2018, todos os relatórios emitidos relatavam ações cibernéticas executadas pela Coreia do Norte. No primeiro relatório a citar tais ações, de 2018, a única atividade observada era referente à espionagem para obtenção de inteligência militar. Nos relatórios seguintes, as ações no espaço cibernético mencionadas também citavam formas que o país estava utilizando para contornar as sanções financeiras impostas pelo conselho, incluindo o uso incremental de criptoativos [157].

Nesse ponto, cabe lembrar que capacidades cibernéticas são assimétricas, e é essa característica que permite a um país como a Coreia do Norte competir contra adversários mais fortes militarmente (JUN *et al.*, 2015, pp. 4-5). Por outro lado, o fato de não ter uma infraestrutura tecnológica tão desenvolvida o transforma, num primeiro momento, em um alvo difícil para ataques ou mesmo retaliações dessa natureza, eventualmente tendo que ser retaliado em outro domínio ou, por exemplo, por meio de sanções econômicas (MANESS, VALERIANO, 2015, p. 93; VAN PUYVELDE, BRANTLY, 2019, p. 134). À medida que se desenvolve tal infraestrutura, aí sim aumenta a superfície de ataque possível de ser explorada pelos adversários. Cabe chamar a atenção para o fato de que os equipamentos que controlavam as centrífugas da usina de Natanz não estavam conectadas à Internet nem a outras redes. Havia uma separação física entre os equipamentos e outros computadores da rede. Ou seja, sua superfície de ataque era mínima. E, ainda assim, o ataque Stuxnet foi executado com sucesso (ZETTER, 2014).

Como Perlroth (2021, p. 335) afirma: "Pyongyang aprendeu que os ataques cibernéticos eram uma forma muito mais fácil de contornar as sanções do que os métodos habituais de falsificação e tráfico ilícito de vida selvagem da Coreia do Norte"[158] (tradução minha). Ela cita inclusive uma fala de Chris Inglis, ex-vice-diretor da NSA entre 2006 e 2014: "o espaço cibernético é um instrumento bastante adequado para eles" porque "[h]á um baixo custo de

[157] Os relatórios são: S/2018/171, S/2019/171, S/2019/691, S/2020/840, S/2021/211, S/2021/777, S/2022/132, S/2023/171, S/2023/656 e S/2024/215. Todos estão disponíveis no sítio: https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports. Acesso em: 25 jun. 2024.

[158] Texto original: "Pyongyang was learning that cyberattacks were a far easier way to get around sanctions than North Korea's usual methods of counterfeiting and illicit wildlife trafficking."

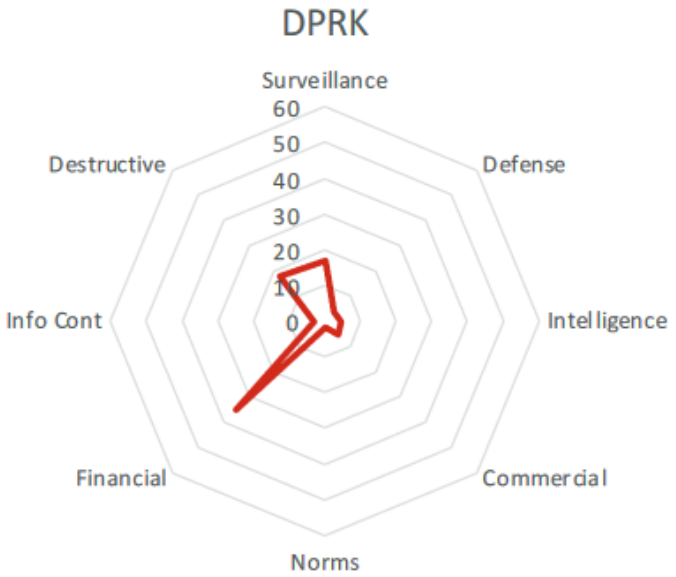
entrada, é bastante assimétrico, há certo anonimato e discrição no seu uso. Pode colocar em risco grandes áreas da infra-estrutura do Estado-nação e da infra-estrutura do sector privado. É uma fonte de renda."[159] Inglis complementa: "[p]odemos argumentar que eles têm um dos programas cibernéticos mais bem-sucedidos do planeta, não porque seja tecnicamente sofisticado, mas porque atingiu todos os seus objetivos a um custo muito baixo"[160] (PERLROTH, 2021, p. 335, traduções minhas). Izycki (2021, p. 53) também afirma que o país não é constrangido por fatores externos para a execução de ações cibernéticas ofensivas (IZYCKI, 2021, p. 53).

Corroborando essa impressão, o relatório de 2022 do *Belfer Center for Science and International Affairs* de Harvard, sobre o cálculo do *National Cyber Power Index* (NCPI), utilizou vários indicadores quantitativos, sendo que para a Coreia do Norte muitos tiveram que ser estimados, o que é esperado dada sua opacidade. O que chamou a atenção foi o alto valor atingido pelo país ao se avaliar o objetivo de "acumular e proteger riqueza". Esse quesito considera que há o objetivo de obter, de forma ilícita, ganhos financeiros utilizando ataques cibernéticos. Nominalmente citam *ransomware* e ataques a infraestruturas físicas de instituições financeiras. Outros objetivos também tiveram alguma pontuação: poder destrutivo e de vigilância, p.ex., mas o de ganhos financeiros deteve maior destaque, como pode ser visto no gráfico de radar apresentado na Figura 10.

[159] Texto original: "There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation-state infrastructure and private-sector infrastructure at risk. It's a source of income."

[160] Texto original: "You could argue that they have one of the most successful cyber programs on the planet, not because it's technically sophisticated, but because it has achieved all their aims at very low cost."

Figura 10 – Gráfico de radar do NCPI para a Coreia do Norte



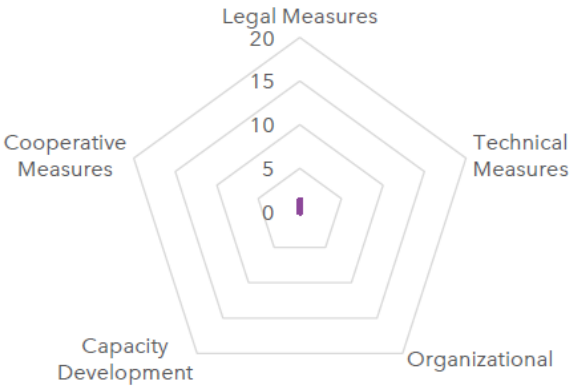
Fonte: Corte da Figura 5.a de Voo *et. al* (2022, p. 22).

Também reforçando essas constatações, o relatório *Global Cybersecurity Index* (GCI) versão 4, de 2020, elaborado pela União Internacional das Telecomunicações (ITU) para auxiliar os países a avaliar sua preocupação com a segurança cibernética, classificou a Coreia do Norte na posição 181, correspondente à última colocação[161] do índice, com o escore de 1,35 (de um total de 100) (ITU, 2020, p. 27). Como curiosidade, a Coreia do Sul apresentou um escore de 98,52 nesse índice, ocupando a primeira posição na região da Ásia-Pacífico (ITU, 2020, p. 29) e a quarta posição mundial (ITU, 2020, p. 25). A título de comparação, a Figura 11 traz o perfil da Coreia do Norte descrito pelo relatório, ao passo que a Figura 12 traz o da Coreia do Sul.

[161] Nesse caso, desconsidero outros três países do índice: Iêmen, Estados Federados da Micronésia e Vaticano. Isso porque não tiveram seus dados coletados e, portanto, têm um escore 0.

Figura 11 – Perfil da Coreia do Norte conforme GCI versão 4

*Democratic People's Republic of Korea***



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures

Area(s) of Potential Growth
Technical, Organizational, Cooperative, Capacity Development Measures

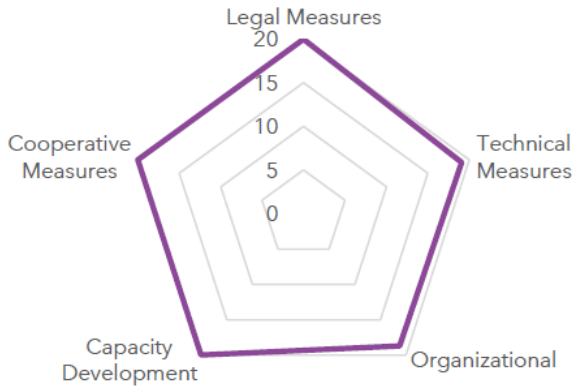
Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
1.35	1.35	0.00	0.00	0.00	0.00

Source: ITU Global Cybersecurity Index v4, 2020

Fonte: ITU (2020, p. 86).

Figura 12 – Perfil da Coreia do Sul conforme GCI versão 4

Korea (Republic of)



Development Level:
Developing Country

Area(s) of Relative Strength
Legal, Cooperative, Capacity Development Measures

Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.52	20.00	19.54	18.98	20.00	20.00

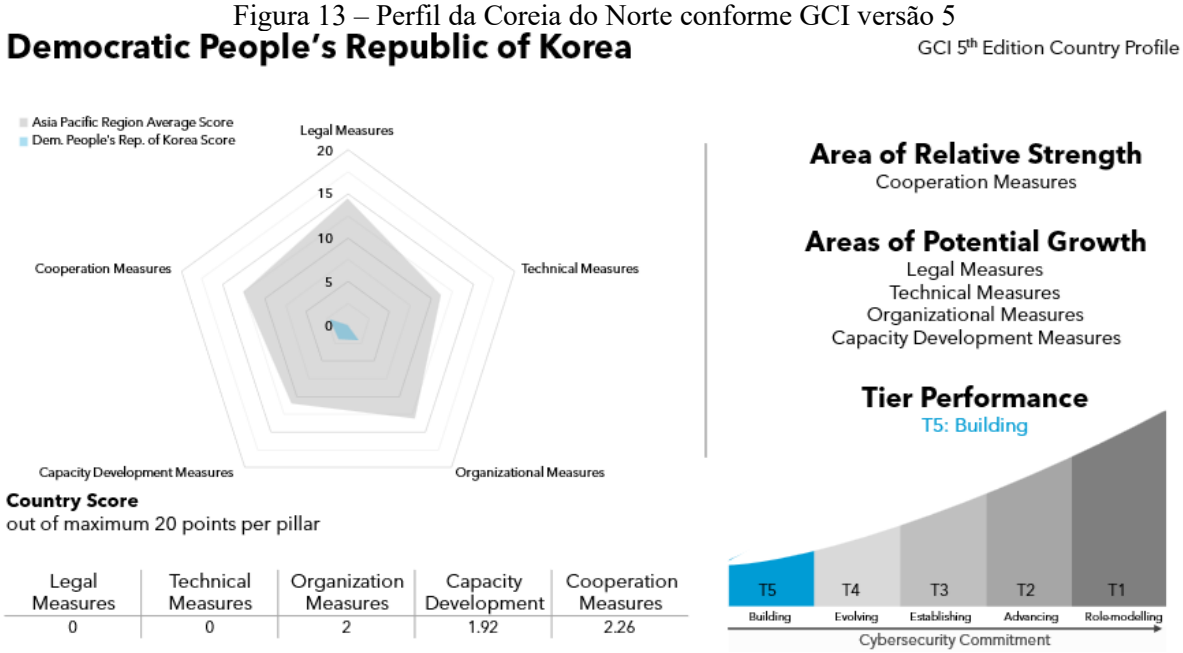
Source: ITU Global Cybersecurity Index v4, 2020

Fonte: ITU (020, p. 89).

Como anteriormente afirmado, em 2024 a ITU lançou a versão 5 do seu relatório do GCI (ITU, 2024), sem diferenças metodológicas significativas (ITU, 2024, pp. 134-137).

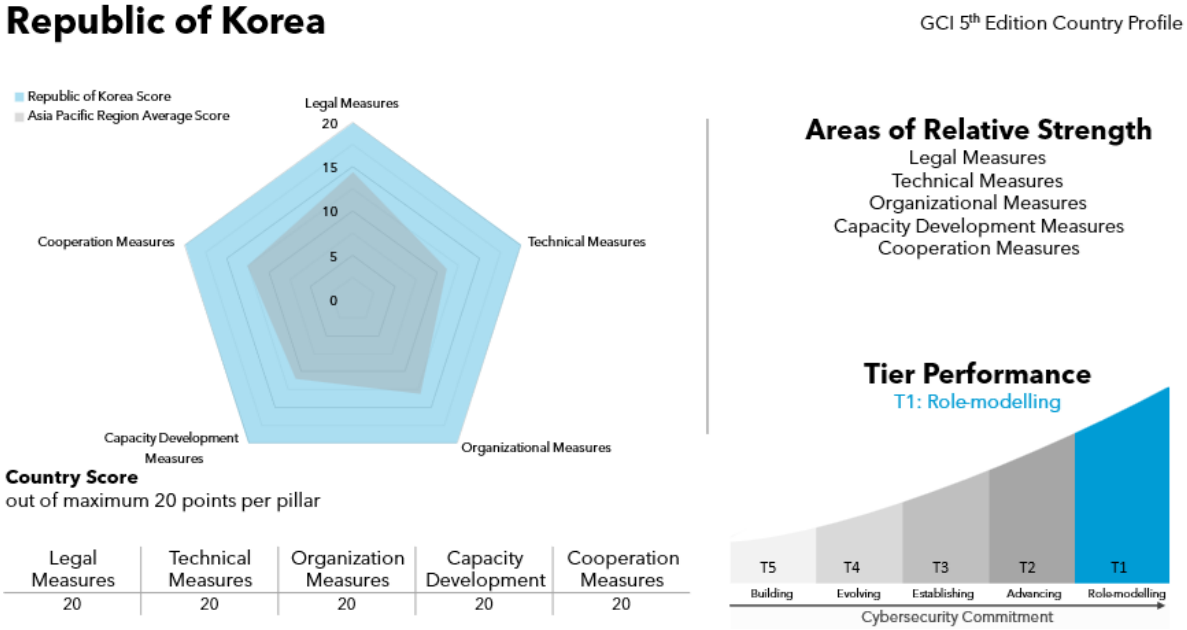
Houve, no entanto, o abandono da classificação (*ranking*) de países havendo, em seu lugar, somente a classificação entre faixas (*tiers*), sendo a primeira (T1) para os países com índices entre 95 e 100, os quais são classificados como países-modelo, com grande comprometimento do governo e ações positivas para a segurança cibernética, e a última (T5) para os países com índices entre 0 e 20, os quais apresentariam comprometimento básico por parte do seu governo quanto à segurança cibernética (ITU, 2024, p. 133). Considerando os novos dados coletados entre 2023 e 2024, a Coreia do Sul se manteve na primeira faixa (T1), ao passo que a Coreia do Norte na última (T5). Os novos perfis da Coreia do Norte e da Coreia do Sul podem ser vistos na Figura 13 e Figura 14, respectivamente.

Figura 13 – Perfil da Coreia do Norte conforme GCI versão 5



Fonte: ITU (2024, p. 84).

Figura 14 – Perfil da Coreia do Norte conforme GCI versão 5



Fonte: ITU (2024, p. 94).

A preocupação com as capacidades cibernéticas que se desenvolvem fez do país um dos quatro citados tanto na Estratégia Cibernética Nacional dos Estados Unidos de 2018, quanto na de 2023. A Estratégia de 2018 afirma que

> Rússia, China, Irã e a Coreia do Norte utilizam o espaço cibernético como meio de desafiar os Estados Unidos, seus aliados e parceiros, muitas vezes com uma imprudência que não considerariam em outros domínios. Estes adversários utilizam ferramentas cibernéticas para minar nossa economia e democracia, roubar propriedade intelectual e semear a discórdia em nossos processos democráticos. Somos vulneráveis a ataques cibernéticos em tempos de paz contra infraestruturas críticas e aumenta o risco de que estes países conduzam ataques cibernéticos contra os Estados Unidos durante uma crise fora de uma guerra. Estes adversários estão desenvolvendo continuamente armas cibernéticas mais novas e eficazes.[162] (EUA, 2018b, pp. 2-3, tradução minha).

O mesmo documento sustenta que Rússia, Irã e Coreia do Norte executam ataques cibernéticos de forma irresponsável, eventualmente prejudicando negócios e aliados do país. E que a China está mais envolvida com espionagem cibernética e furto de propriedade intelectual (EUA, 2018b, pp. 1-2).

[162] Texto original: "Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons."

Na Estratégia publicada em 2023, a Coreia do Norte é citada como um estado que utiliza suas capacidades cibernéticas contra os interesses dos EUA, as normas internacionais e direitos humanos, ameaçando a segurança nacional do país e sua prosperidade econômica (EUA, 2023a, p. 7). Inclusive, no documento, chega-se a afirmar algumas das formas como o país se utiliza de tais capacidades:

> Os governos do Irã e da República Popular Democrática da Coreia (DPRK) estão crescendo igualmente na sua sofisticação e vontade de realizar atividades maliciosas no ciberespaço. O Irã tem utilizado capacidades cibernéticas para ameaçar os aliados dos EUA no Oriente Médio e outros lugares, enquanto a DPRK **realiza atividades cibernéticas para gerar receitas** tanto por meio de empresas criminosas, como do furto de criptomoedas, *ransomware* e da implantação de trabalhadores clandestinos de tecnologia da informação (TI) com **o objetivo de alimentar as suas ambições nucleares**. O amadurecimento adicional destas capacidades poderá ter impactos significativos nos interesses dos EUA, seus aliados e parceiros[163] (EUA, 2023a, p. 3, tradução e grifos meus).

Exemplos dessas capacidades incluem, por exemplo, a interferência de sinais eletrônicos contra armas guiadas dos EUA e Coreia do Sul, observada durante exercícios militares entre os dois países (SANGER, BROAD, 2017), bem como aeronaves civis que sofreram interferência de sinais do *Global Positioning System* (GPS) durante a sua navegação em diversas oportunidades desde 2010 (SANG-HUN, 2016).

Quanto à inteligência artificial (IA), a Coreia do Norte pode usá-la para afiar sua "espada de múltiplos propósitos", tanto para ações ofensivas cibernéticas quanto defensivas, assim como qualquer nação atualmente faz. Entretanto, na interpretação dos autores de um estudo de 2022, o país ainda não estaria utilizando tal tecnologia (HAROLD *et al.*, 2022, p. 17). Chamo a atenção para o fato de que, desde 2022, os avanços da IA foram substanciais e, provavelmente, o fio da espada já esteja sendo muito bem afiado. Tanto que o relatório mais recente da Agência da União Europeia para a Cibersegurança (ENISA) cita que grupos de ataques cibernéticos ofensivos associados a Estados, como os da Coreia do Norte, já estariam utilizando funcionalidades de ferramentas de IA conhecidas e disponíveis de forma aberta para qualquer usuário (ENISA, 2024, p. 25). Por outro lado, um relatório da Microsoft (2024b) de 2024, por sua vez, não identificou tais usos.

---

[163] Texto original: "The governments of Iran and the Democratic People's Republic of Korea (DPRK) are similarly growing in their sophistication and willingness to conduct malicious activity in cyberspace. Iran has used cyber capabilities to threaten U.S. allies in the Middle East and elsewhere, while the DPRK conducts cyber activities to generate revenue through criminal enterprises, such as through the theft of cryptocurrency, ransomware, and the deployment of surreptitious information technology (IT) workers for the purposes of fueling its nuclear ambitions. Further maturation of these capabilities could have significant impacts on U.S., allied, and partner interests."

5.2 Usos ofensivos

Conforme Sanger (2018, p. 136) demonstra, o desenvolvimento de capacidades cibernéticas ofensivas (ele usa o termo *cyberweapons*) é algo bastante interessante para a Coreia do Norte, já que se trata de um país isolado, bastante sancionado, incapaz de se sustentar num conflito contra outras potências e com muito pouco a perder. Kello (2017, pp. 154-155), por sua vez, cita como três os objetivos do programa cibernético norte-coreano: ofensivo, psicológico e, por fim, coerção e político.

Relatórios afirmam que o país começou a se estruturar para empreender ações cibernéticas em 2009. Em julho desse ano executou os primeiros ataques de DDoS contra sítios governamentais sul-coreanos, demonstrando que estava explorando as possibilidades deste espaço e construindo um arsenal cibernético diversificado, forjando sua "espada de múltiplos propósitos" (RECORDED FUTURE, 2023; NOVETTA, 2016; JUN *et al.*, 2015; KONG, 2019).

Microsoft (2022) aponta que os Estados Unidos seriam o principal alvo de ataques cibernéticos oriundos de grupos da Coreia do Norte, seguido pela Coreia do Sul, com o primeiro tendo sido alvo de 38% dos ataques e o segundo, 8% deles (medidos entre julho de 2021 e junho de 2022) (MICROSOFT, 2022). O relatório de 2023 (julho de 2022 a junho de 2023) já demonstra 41% dos ataques destinados aos EUA e 15% à Coreia do Sul, ou seja, mais de 50% dos ataques registrados originários da Coreia do Norte dirigiram-se a esses dois países (MICROSOFT, 2023). O relatório da Microsoft de 2024 não separa por país, mas por região. Segundo ele, a Coreia do Norte direciona 54% dos ataques à América do Norte, 18% à Ásia Oriental & Pacífico e 18% à Europa e Ásia Central (MICROSOFT, 2024).

A parceira Rússia também já foi alvo de ataques recentes dos APT ScarCruft e Lazarus, associados à Coreia do Norte. Em 2022 houve uma invasão da rede da empresa NPO Mashinostroyeniy (ou NPO Mash), detentora de tecnologias para desenvolvimento e fabricação de mísseis hipersônicos, satélites e armamentos balísticos de nova geração, possivelmente para espionagem (PEARSON, BING, 2023; HEGEL, 2023). O ministério das relações exteriores russo também já teria sido espionado pelos norte-coreanos (KANG, 2024). Durante a pandemia de COVID-19, houve relatos sobre tentativas de invasões a sistemas de empresas russas que desenvolviam vacinas contra o vírus (STUBBS, 2020; JEONG, 2020).

Na base de dados *Cyber Operations Tracker* do *Council on Foreign Relations* (CFR), entre 2005 e 2023, a Coreia do Norte foi identificada como responsável por 109 das 897 operações registradas, ou seja, pouco mais de 12%. Destaca-se que se trata de ações cuja origem

foi inequivocamente identificada como sendo da Coreia do Norte. A Tabela 1 quantifica os ataques executados pelo país, de acordo com a citada base, conforme seu objetivo.

Tabela 1 – Ações cibernéticas da Coreia do Norte, por objetivo, conforme *Cyber Operations Tracker* (entre 2005 e 2023)

Tipo	Quantidade
Espionagem	73
Furto	24
Negação de serviço	4
Doxing[164]	2
Destruição de dados (sabotagem)	1
Não identificado	5

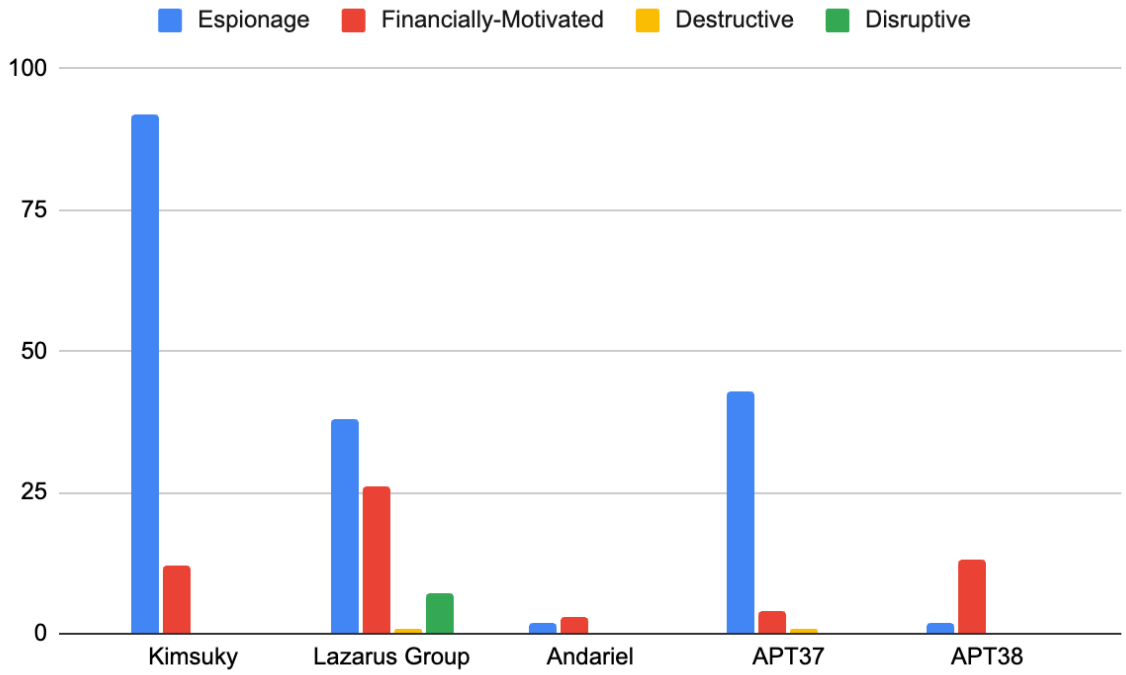
Fonte: elaboração própria com base no *Cyber Operations Tracker* do CFR.

Outro levantamento foi o feito por Izycki (2021, pp. 40, 44), que considerou informações até 2020, agregando outras bases de dados além da *Cyber Operations Tracker* citada. Segundo ele, a Coreia no Norte teve como alvos os seguintes setores: governamental, militar, aeroespacial e de criptoativos. Nesse caso, ele classificou seus objetivos como: crimes cibernéticos (financeiros), espionagem, sabotagem e disrupção (*disruption*), demonstrando a ampla gama de propósitos que move o país.

Em 2023, a Recorded Future analisou uma base de dados (coletados pela empresa) de ações ofensivas atribuídas a cinco grupos associados à Coreia do Norte: Lazarus, APT38, Andariel, Kimsuky e APT37. Segundo a empresa, os grupos APT38 e Andariel seriam subgrupos do Lazarus, e o APT37 possui TTP bastante semelhantes aos do Kimsuky, aparentemente pelo fato de os objetivos serem semelhantes (RECORDED FUTURE, 2023). A separação em grupos neste estudo não é tão relevante, principalmente porque, no fim, são todos atuando pelo regime norte-coreano. Para o estudo quantitativo realizado, entretanto, a separação era interessante. Este contabilizou as atividades de cada grupo por ano, por tipo e localização de alvos, objetivo da ação, dentre outros. Apresento aqui dois resultados interessantes, um deles apresentados na Figura 15.

[164] Divulgação de dados pessoais.

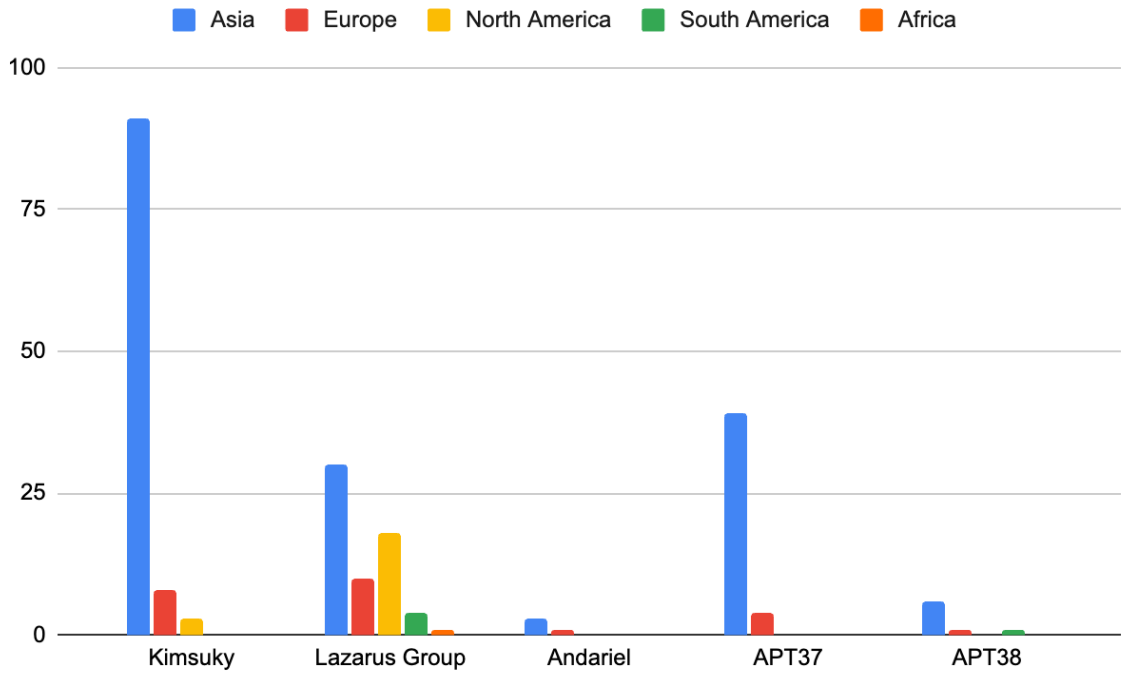
Figura 15 – Quantidade de ataques cibernéticos classificados por objetivo, separados conforme o grupo perpetrador



Fonte: Figura 8 de Recorded Future (2023, p. 14).

Nota-se que cada grupo aparenta ter um objetivo principal. As atividades dos grupos Kimsuky e APT37 têm como propósito primordial a execução de ações voltadas para a espionagem, o que pode explicar o compartilhamento de vários TTP semelhantes. Ainda, esse tipo de atividade é muito mais recorrente do que aquelas com motivação financeira, as quais em que o grupo Lazarus e seu subgrupo APT38 seriam especialistas. Combinando essas informações com as mostradas na Figura 16, nota-se que estão na Ásia os principais alvos das campanhas de espionagem.

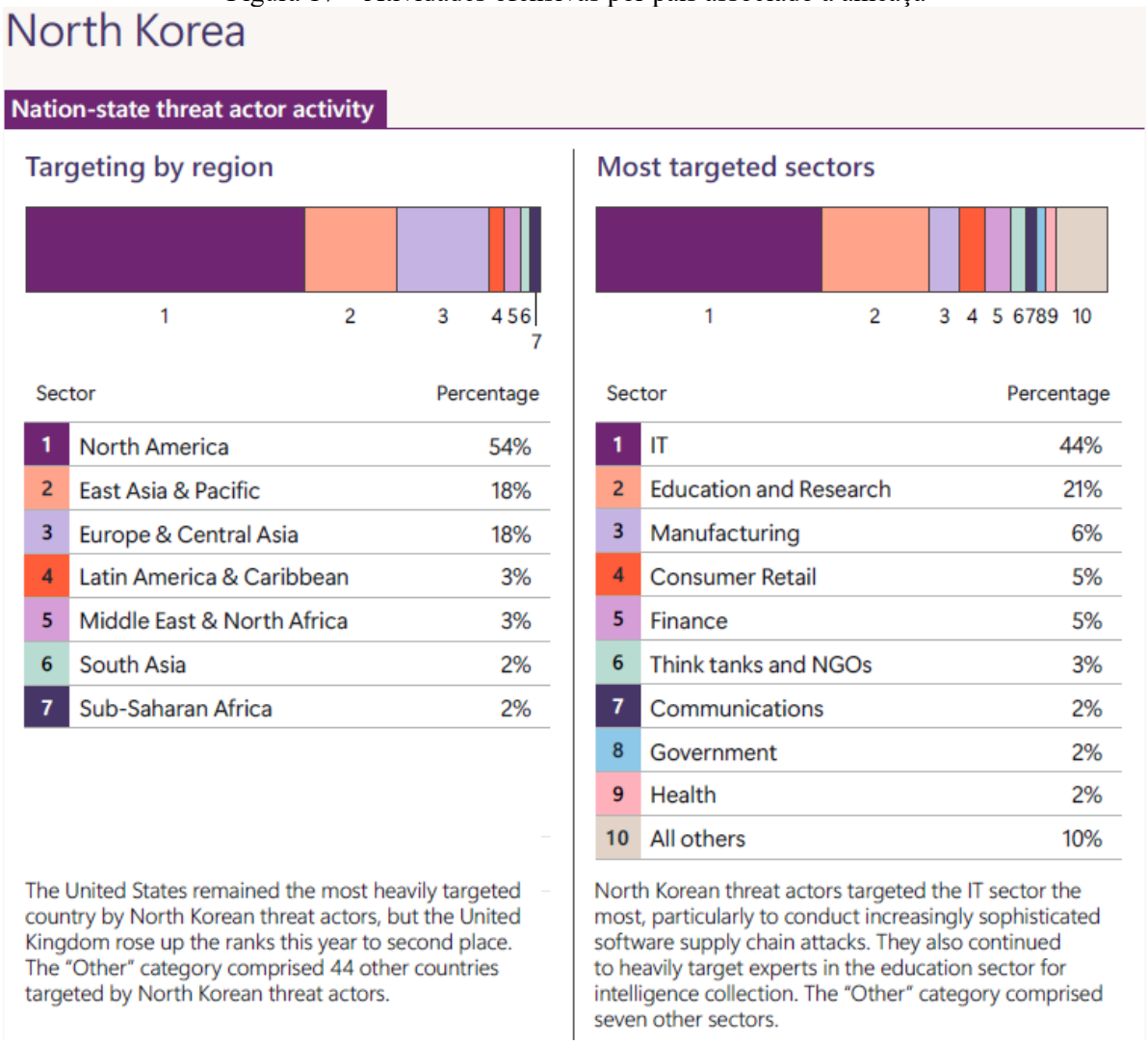
Figura 16 – Quantidade de ataques cibernéticos classificados por região geográfica do alvo, separados conforme o grupo perpetrador



Fonte: Figura 10 de Recorded Future (2023, p. 15).

Um bom resumo de operações executadas pelo Lazarus até 2014 foi elaborado por Novetta (2016, pp. 20-23). A Microsoft (2024a) afirma, justamente, que diversos grupos por eles identificados compartilham táticas consideradas incomuns, sugerindo que há um compartilhamento de conhecimento e TTP entre os atores norte-coreanos. A Figura 17 mostra de forma gráfica a análise dos ataques identificados como sendo de atores norte-coreanos, separados por região e por setores alvo.

Figura 17 – Atividades ofensivas por país associado à ameaça



Fonte: Microsoft (2024b, p. 15).

A seguir, alguns ataques atribuídos a grupos APT associados à Coreia do Norte. Não se trata de uma avaliação completa e aprofundada de todas as ocorrências, porque há muito material já escrito sobre eles. Também não são relacionados itens muito técnicos, visto que competentes empresas já elaboraram relatórios bastante completos, alguns dos quais são referenciados.

5.2.1 Ataque à Sony Pictures Entertainment

A partir dos ataques executados contra a empresa Sony Pictures Entertainment no final de 2013, também chamados de *Sony Hack* ou Operação Blockbuster, Estados e empresas de segurança cibernética passaram a prestar mais atenção nas capacidades cibernéticas da Coreia do Norte. Kello (2017, p. 155-156) e Buchanan (2020, pp. 167-186) explicam sobre o uso deste

ato como de coerção. Buchanan vai além, estudando como é sinalizar para adversários por meio de ações cibernéticas e relacionando alguns dos problemas envolvidos.

Esse caso, incluindo suas questões técnicas, já foi documentado e discutido por diversos autores (NOVETTA, 2016; CORERA, 2015, pp. 301-303, PERLROTH, 2021, p. 276-278; SANGER, 2018, pp. 124-151; BUCHANAN, 2020, pp. 167-186; WHITE, 2020, pp. 72-78; SEGAL, 2017, pp. 57-64; JUN *et al.*, 2015). Em 27 de junho de 2014, o embaixador da DPRK na ONU relatou que *trailers* do filme *The Interview* geraram violentas reações de ódio e fúria em seu país (WHITE, 2020, p. 72). Trata-se de um filme de comédia, produzido e ainda a ser lançado pela Sony, que ironizava um ditador caricaturado como Kim Jong-un e seu assassinato, encomendado pela CIA (BUCHANAN, 2020, p. 167). Tendo a Sony insistido em manter a divulgação da película, o atacante executou um tipo de coerção digital (VALERIANO *et al.*, 2018, pp. 30-31; KELLO, p. 154).

Em 24 de setembro, um trabalhador da Sony teria clicado num *link*, recebido por e-mail, para assistir a um vídeo. A mensagem, na realidade, consistia em parte de uma técnica de ataque de *spearphishing*. Ao clicar, o que ocorreu foi a instalação de um programa na sua máquina, o qual serviu como porta de entrada à rede da empresa. Tal programa implementou a sua persistência na máquina, ou seja, se ela fosse reiniciada, a porta ainda estaria aberta para os invasores, os quais seguiram explorando a rede da organização e invadindo outros sistemas, além de extraírem arquivos internos da empresa, transferindo-os para servidores na Internet sob seu controle.

No dia 21 de novembro, os invasores já estavam há quase dois meses com bastante conhecimento sobre a rede da firma, bem como acesso praticamente irrestrito a ela. Nesse dia, um grupo supostamente intitulado “God’sApstls” enviou e-mails para cinco diretores da companhia com ameaças de ataque, sem especificar o que seria, exigindo dinheiro. Nos dias 22 e 23 seguintes, um novo código malicioso, que recebeu o nome de Destover, foi executado nas máquinas na rede da Sony que foram invadidas. Os códigos executavam a técnica de apagamento das mídias de armazenamento, de forma similar à usada em ataque do Irã contra a empresa saudita Saudi Aramco, em 2012, porém tinham maior poder de dano. Por fim, em cada computador aparecia uma tela com um esqueleto e o texto “Hacked by #GOP”, sendo que esta seria a abreviação do suposto grupo, *Guardians of Peace* (Guardiões da Paz). Além disso, um texto maior informava que o grupo teria se apoderado de arquivos, exigindo o cumprimento das suas ordens, sem especificar quais seriam.

Em 8 de dezembro daquele ano, uma nova ameaça foi encaminhada solicitando que o “filme de terrorismo” não deveria ser projetado, o qual “poderia quebrar a paz regional e causar

a guerra!" (BUCHANAN, 2020, p. 178). O fato é que, no mesmo dia, a empresa teve grande quantidade de arquivos vazados, entre vídeos completos de filmes, roteiros ainda por lançar, bem como arquivos internos como contratos, salários e e-mails privados, por exemplo. O dano à imagem da empresa foi significativo, incluindo insatisfação de funcionários e artistas, que descobriram suas diferenças salariais e de cachês, além de apelidos ou adjetivações inadequadas, usadas por colegas e superiores, em mensagens trocadas. Somado a isso, ameaças foram feitas a cinemas que projetassem o filme, citando o ataque terrorista de 11 de setembro. O receio de tal ataque desmotivou diversas salas a projetá-lo, e a Sony suspendeu seu lançamento. Eventualmente, no dia de Natal daquele ano, o filme foi exibido em cinemas independentes, além de ter sido disponibilizado *online* (NOVETTA, 2016; CORERA, 2015, pp. 301-303, PERLROTH, 2021, p. 276-278; SANGER, 2018, pp. 124-151; BUCHANAN, 2020, pp. 167-186; WHITE, 2020, pp. 72-78; SEGAL, 2017, pp. 57-64; JUN *et al.*, 2015).

A atribuição foi relativamente simples, já que, dentre outros indícios, os atacantes teriam utilizado a mesma base de ataque usada contra bancos e empresas de mídia em 2013. Além disso, nome "Guardians of Peace" nunca tinha sido registrado em ações antes (nem depois), não se tratando de algo crível. Poucos dias depois do ataque, o presidente Obama acusou diretamente a Coreia do Norte, sugerindo que os EUA retaliariam à altura (WHITE, 2020, p. 75; PERLROTH, 2021, p. 278; GREENBERG, 2019, p. 112; WHITE, 2020, p. 75). Perlroth (2021, p. 278) ainda acrescenta que a declaração do presidente seria tanto como sinalização para aquele país quanto para o Irã.

Ao final, entretanto, o filme, que teria qualidade questionável, não alcançaria tanto sucesso se não houvesse tal ataque, a mídia espontânea que gerou e a polêmica que o envolveu. Ele foi muito assistido e virou praticamente um bastião da liberdade de expressão. Na interpretação de Buchanan (2020, pp. 184-186), após as ameaças da Coreia do Norte e diante da negativa da Sony em cancelar o filme, o país passou a executar a coerção no ambiente internacional, mas aplicada ao meio digital. A sinalização do desejo dos norte-coreanos não surtiu o efeito direto esperado. Mas a operação mostrou que ações cibernéticas poderiam, se bem executadas, ser utilizadas para este fim (BUCHANAN, 2020, pp. 307-312; VALERIANO *et al.*, 2018, pp. 30-31). No entanto, resultados indiretos foram obtidos, como o fato de que outros estúdios cancelaram projetos que pudessem ofender o regime norte-coreano (KELLO, 2019, p. 156; BUCHANAN, 2020, p. 186).

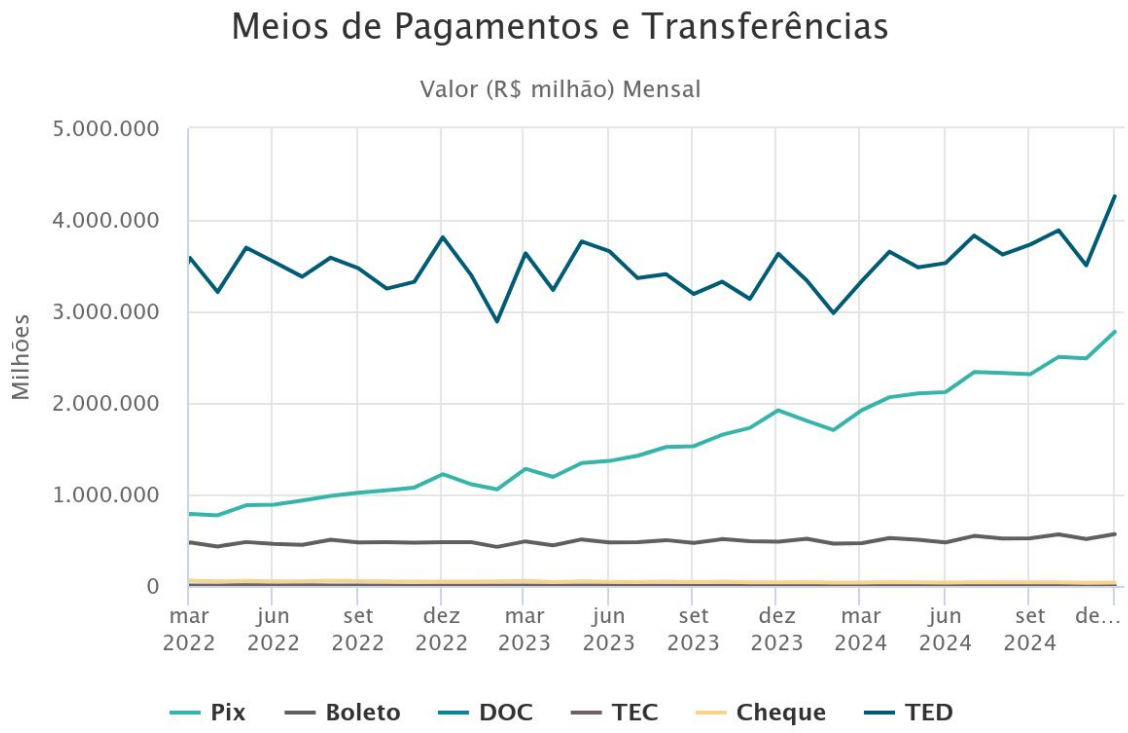
Com relação às retaliações prometidas, elas nunca ocorreram à altura, como foi dito. A lista de sanções foi ampliada, algumas sem relação com o assunto. A pós investigações deste caso, como foi identificado um indivíduo a quem pudesse ser atribuídas as ações cibernéticas,

foi feita uma representação criminal à justiça estadunidense (BUCHANAN, 2020, p. 183; EUA, 2018a). Mais à frente isso é explicado.

5.2.2 Ataques a bancos e corretoras

Uma forma comum de se obter dinheiro em espécie é por meio de assaltos a bancos, o que – como mostra a história – já ocorreu em todo o mundo. O uso incremental de sistemas computacionais em atividades e empresas, inclusive bancos, permitiu que esse crime deixasse de ser uma ação que envolve armas de fogo, sequestros ou fugas espetaculares. Possíveis ataques a redes de bancos já são preocupações há anos, inclusive de manipulação de dados em operações bancárias (KAPLAN, 2016, p. 175; SCHNEIER, 2018, pp. 81-82). Pagamentos entre empresas ou pessoas físicas passam por esses sistemas, hoje, a cada segundo, sempre por intermédio do sistema de algum banco. No Brasil, as estatísticas do Banco Central sobre o uso dos meios de pagamentos mostram que os valores enviados por Transferência Eletrônica Disponível (TED) e PIX, ambos eletrônicos, atingiu R$ 4,26 trilhões e R$ 2,78 trilhões, respectivamente, em dezembro de 2024. O gráfico da Figura 18, com valores mensais conforme o meio de transferência usado, de março de 2022 a dezembro de 2024, mostra, inclusive, a tendência ascendente de uso do PIX.

Figura 18 – Comparação mensal do volume financeiro, por instrumento de pagamento



Fonte: Banco Central do Brasil[165].

A rede SWIFT (do inglês, *Society for Worldwide Interbank Financial Telecommunication*) é uma rede à qual instituições financeiras de todo o mundo se conectam para executar transferências monetárias entre si. As operações são solicitadas de forma eletrônica através do envio de mensagens por meio dessa rede e seus sistemas.

O furto de bancos na forma de transações eletrônicas entre uma conta de origem (furtada) e outra de destino (à qual o criminoso tem acesso) passa a não mais ser uma atividade com diversos riscos, como um assalto à agência bancária, envolvendo o uso irregular de um sistema computacional que envolveria conhecimento (por vezes bastante aprofundado) das TIC e da burocracia bancária, como o conhecimento da rede SWIFT e sua operação, por exemplo.

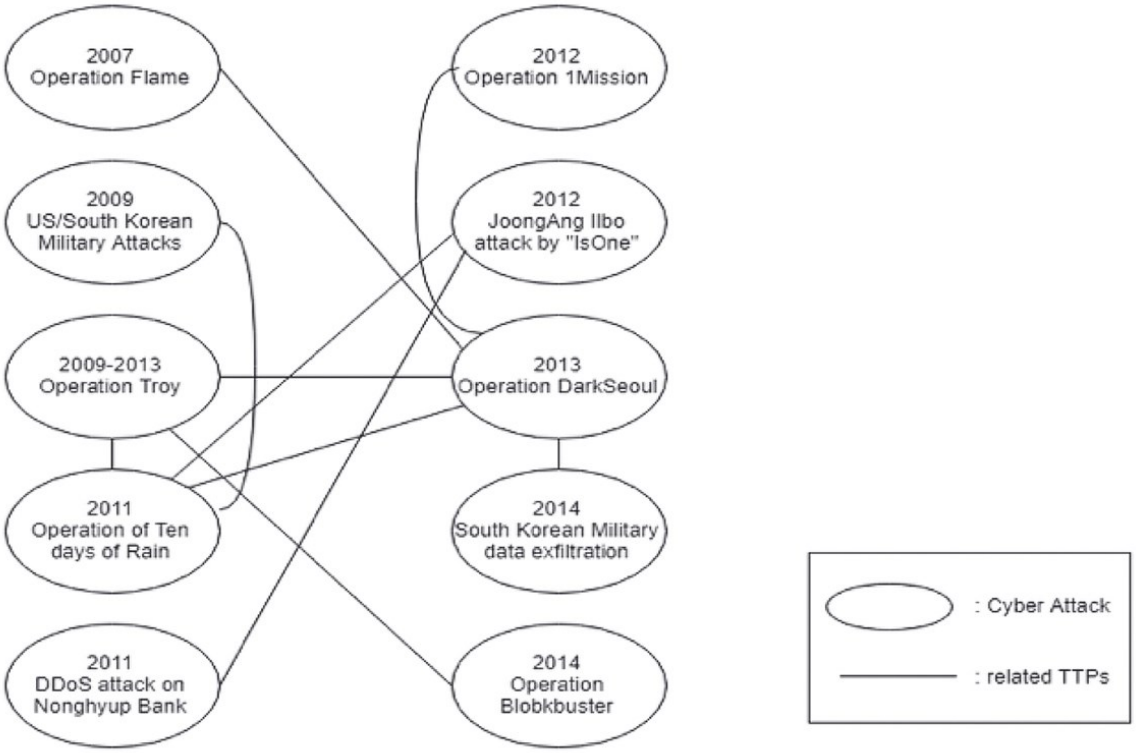
A Coreia do Norte percebeu que esse também era um caminho a ser seguido. Tais crimes cibernéticos teriam o objetivo financeiro de sustentar o regime norte-coreano e o desenvolvimento das armas de destruição em massa (DNI, 2024, p. 22). Em 2011, executou ataques contra a Coreia do Sul direcionados a sistemas de infraestruturas críticas, mídia e instituições financeiras. Estes últimos, ainda sem o propósito financeiro, envolvendo

[165] Imagem gerada a partir dos relatórios do Banco Central do Brasil em: https://www.bcb.gov.br/estatisticas/detalhamentoGrafico/graficosspb/MeiosPagamentosValor. Acesso em: 28 jan. 2025.

sabotagem, chegando a inutilizar 273 de 587 dos equipamentos servidores de um só banco (46,5%). Em 2012 o país atacou outra organização de mídia. Em março de 2013 foi a vez da operação Dark Seul, com ataques contra agências de notícias e bancos, cujo resultado foi o apagamento dos dados de um total de 48 mil equipamentos das empresas alvo. Esse ataque foi oficialmente atribuído à Coreia do Norte pela Coreia do Sul, que apresentou evidências técnicas na acusação (BUCHANAN, 2020, p. 169, KU, 2021, p. 268; KONG *et al.*, 2019, p. 9-10; KIM, POLITO, 2019).

Kong *et al.* (2019, p. 10-11) analisaram os TTP de 10 operações (algumas das quais são citadas aqui) e elaboraram o grafo da Figura 19. Cada nó (elipse) do grafo é uma operação ofensiva cibernética, com o ano em que foi realizada e o nome pelo qual é mais comumente chamada. As arestas (linhas) indicam que há compartilhamento de TTP entre as operações. Percebe-se que todos os ataques apresentam ao menos uma conexão com outro ataque.

Figura 19 – Relacionamentos entre ataques cibernéticos entre 2007 e 2012 com base na comparação entre os TTP



Fonte: Figura 6 de Kong *et al.* (2019, p. 10).

O fato de não haver uma retaliação significativa após os ataques de 2014 contra a Sony pode ter servido de incentivo para o país buscar outras atividades, já que, a partir do ano de 2015, as ações cibernéticas ofensivas contra bancos passaram a ter objetivo financeiro. Houve tentativas de invasão em um banco das Filipinas e de um banco do Vietnã. Neste último,

tentaram executar uma transferência fraudulenta utilizando a rede SWIFT, a qual foi identificada e não executada (WHITE, 2020, p. 62).

O grupo Lazarus, no início de 2016, executou uma operação bastante complexa contra o Banco Central de Bangladesh. O objetivo aparente era transferir e sacar US$ 1 bilhão das contas do banco, por meio de um engenhoso esquema previamente planejado. Assim como no caso da Sony, sobre este também já há várias publicações (WHITE, 2022; WHITE, 2020, pp. 66-96; DAS, SPICER, 2016; BUCHANAN, 2020, pp. 271-275). Outra fonte bastante rica de informações é o processo movido pelos EUA contra Jin Hyok Park (EUA, 2018a). O jornalista investigativo Geoff White pesquisou a fundo o ocorrido, chegando a publicar um *podcast* e, posteriormente, um livro sobre o caso, ambos com o nome *The Lazarus Heist*[166]. Trata-se de um caso interessante pela sua transnacionalidade e por ter envolvido o banco central de um país.

O ataque, na verdade, iniciou em janeiro de 2015, quando um anexo malicioso foi encaminhado a funcionários do Banco de Bangladesh (ataque de *spearphishing*). Um dos destinatários abriu e teve seu computador infectado. Através deste, os invasores conseguiram vasculhar e infectar outros equipamentos da rede do banco, executando o movimento lateral, até chegar àqueles responsáveis pelas transações internacionais por meio da rede SWIFT. Para a execução do ataque, além da invasão dos sistemas bancários, era necessário fazer várias ações prévias, como a criação de contas internacionais para onde os valores seriam transferidos através do sistema SWIFT.

Mais de um ano depois do primeiro acesso à rede do banco, às 20:36 do dia 4 de fevereiro de 2016 foram encaminhadas 36 transações pela rede SWIFT, solicitando totalizando US$ 951 milhões, da conta do Banco de Bangladesh no Federal Reserve (banco central dos EUA) para diversas contas em outros países. Todas as transações foram negadas automaticamente devido a um erro de formatação. Erro consertado, reencaminharam as mesmas transações, todas elas direcionadas a pessoas físicas. Os invasores também alteraram o funcionamento de uma impressora laser que, para cada operação na rede SWIFT do banco, imprimia uma página com os dados, transformando-se num registro analógico. Às 3:59 do dia seguinte, os invasores se desconectaram da rede e da máquina, apagando seus rastros.

Nem todas as 36 transferências foram executadas. Um banco de Sri Lanka identificou a transferência como suspeita, notificando o Federal Reserve que, em seguida, cancelou das demais transações. O Banco de Bangladesh também foi notificado e buscou cancelar as

[166] O podcast, original em inglês, está disponível gratuitamente em: https://www.bbc.co.uk/programmes/w13xtvg9/episodes/downloads.

transferências executadas entrando em contato com os demais bancos. Alguns contatos não tiveram sucesso, porque foram depositados em contas que, em seguida, tiveram os fundos transferidos para outros bancos, por vezes de outros países, e sacado ou utilizado em cassinos, uma forma bastante usada para lavar dinheiro ilegal. No total, o banco bengali perdeu US$ 81 milhões.

A maior parte do dinheiro chegou a contas de um banco filipino, abertas em situações suspeitas. No meio do processo, transferiram parte do valor para outras instituições, parte foi sacada e parte foi enviada para dois cassinos em Manila. Nos cassinos, os valores foram apostados em mesas de bacará e, o que restou, transferido para outras mãos, terminando na Coreia do Norte, segundo a investigação conduzida pelo FBI WHITE, 2022; WHITE, 2020, pp. 66-96; DAS, SPICER, 2016; BUCHANAN, 2020, pp. 271-275).

White (2020, p. 92) chama a atenção para o fato de que os criminosos, durante a execução dos atos, se cadastraram em de empresas dos EUA, criando contas para se comunicar, como Google e Facebook. Com isso, a polícia estadunidense conseguiu, via processo judicial, cumprir 100 mandatos de busca e apreensão para 1000 contas de e-mail e perfis de redes social, além de emitir 85 solicitações formais de evidências a outros países por meio de Auxílio Direto (MLA) (EUA, 2018a, p. 2). Ainda que se possa solicitar auxílio direto entre países, quando se trata de empresas nacionais, mandados judiciais locais são sempre mais ágeis na execução e só dependem da legislação do país. Isso é o equivalente ao que a NSA, quando chama de "vantagem de mando de campo" (*home-field advantage*): como em um jogo onde a torcida está toda a seu favor (BUCHANAN, 2020, p. 15).

Em 2018, um ataque diferente foi feito contra o banco indiano Cosmos Bank, que recebeu o nome de FASTCash. Como um dos problemas enfrentados nas operações anteriores era sacar o dinheiro em espécie, estruturaram um ataque que não dependessem mais de transações SWIFT, o dinheiro seria sacado direto nos terminais de autoatendimento. Em junho de 2018 invadiram a rede do banco e, em 11 de agosto, inseriram no sistema um código que sobrepunha a autenticação de senha em saques. Em pelo menos 28 países executaram operações com cartões clonados, sacando quantias entre US$ 100 e US$ 2.500, sem a necessidade de uso de senha. Foram mais de 2.800 na Índia e mais de 12.000 operações fora do país. Em duas horas foram retirados mais de US$ 10 milhões do banco. Dois dias depois, ainda com acesso ao sistema do banco, transferiram US$ 2 milhões para uma conta em Hong Kong via SWIFT. Após o incidente, os sistemas foram retirados do ar por pelo menos nove dias. O Painel de Peritos da ONU atribuiu o ataque ao APT38, subgrupo do Lazarus. Em 2023, na Índia, onze pessoas foram

julgadas culpadas do crime, todos envolvidos com os saques e nenhum com a invasão aos sistemas (BUCHANAN, 2018, pp. 284-287; KREBS, 2018; SHAIKH, 2018; ONU, 2019).

Após a ação contra os bancos, um tipo de ataque surgia e o grupo Lazarus teria se especializado eram os do tipo *ransomware*. O ataque WannaCry foi um dos mais marcantes por alguns motivos. Iniciado em 12 de maio 2017, ele foi um dos mais agressivos até então, afetando 200 mil organizações em 150 países somente em 24 horas, sendo que os países mais atingidos foram China e Rússia[167]. Outro motivo foi o uso de uma ferramenta de nome ETERNALBLUE, uma das criadas pela NSA e distribuída pelos Shadow Brokers, que explorava uma falha do sistema operacional Windows XP, recentemente corrigida pela Microsoft em março de 2017. A correção para a falha ainda não estava aplicada a todos os computadores, e a ferramenta tinha uma capacidade de exploração muito rápida. Assim que um computador era invadido usando tal falha, os desenvolvedores já o programaram para buscar novos computadores em seguida. Uma rede local com algumas centenas de computadores era toda infectada em poucos segundos. Assim que infectada, outra ferramenta executada na máquina criptografava aos arquivos da máquina, cobrando resgate para fornecerem a chave. Entretanto, ainda que o usuário pagasse, não haveria como recuperar os arquivos porque a chave não seria fornecida.

Análises técnicas permitiram concluir, em pouco tempo, que o WannaCry era um produto do grupo Lazarus, por conter várias coincidências com ataques anteriores, como aqueles ao Banco de Bangladesh e à Sony. Entretanto, só em dezembro de 2017 os EUA e Reino Unido atribuíram formalmente sua autoria ao país asiático (BUCHANAN, 2020, p. 280; PERLROTH, pp. 333-336; SANGER, 2018, pp. 288-291; WHITE, 2020, pp. 96-127).

Uma forma encontrada de retaliar foi usar o comumente chamado de *naming and shaming* de seus operadores. Nos EUA, tem sido comum o uso de processos legais envolvendo não o país que tenha executado alguma atividade cibernética contra eles, mas sim as pessoas físicas identificadas como sendo os executores da ação ou, de alguma forma, envolvidos no caso. Isso tem ocorrido com chineses, russos e norte-coreanos. Num caso da Coreia do Norte, os Estados Unidos processaram na Justiça Jin Hyok Park (outros possíveis nomes: Pak Jin Hek, Pak Kwang Jin) (EUA, 2018a; WHITE, 2022). O mesmo indivíduo estaria relacionado com outros furtos, como o do Banco de Chile e do Cosmos Bank da Índia (ONU, 2019).

[167] A explicação curiosa é que era comum usarem programas piratas, os quais não recebiam correções para falhas de segurança como a que foi explorada nesse ataque.

A Coreia do Norte nega todas as acusações, afirmando serem parte de uma campanha de difamação dos EUA contra o país (WHITE, 2020, pp. 66-96; WHITE, 2022; BUCHANAN, 2020, pp. 271-275; SANGER, 2018, pp. 285-286; CARLIN, 2018, p. 401).

Em 2015, antes do Banco de Bangladesh, outros bancos também sofreram ataques: um ataque a um banco do Equador rendeu US$ 100 milhões. No mesmo ano, não tiveram a mesma sorte em bancos do Vietnã e Filipinas (WHITE, 2020, p. 93).

Entre 2016 e 2018 ocorreram ataques (ou tentativas) do mesmo tipo em outras instituições de grande porte e relevância, como o Banco Mundial, Banco Central Europeu, Bank of America, Deutsche Bank. Além destes, ocorreram tentativas em ao menos vinte bancos poloneses, outros no México, Uruguai e África. Em 2016 invadiram o sítio da Internet do órgão financeiro regulador da Polônia, através do qual chegaram a infectar usuários que os acessaram, vindos dos bancos centrais de Venezuela, Estônia, Chile, Brasil e México. Em outubro de 2017 conseguiram US$ 60 milhões de um banco em Taiwan, e em 2018, US$ 10 milhões do Banco de Chile (MOZUR, SANG-HUN, 2016; SANGER, 2018, p. 286; WHITE, 2020, p. 93; ONU, 2019).

Mais recentemente, alguns dos crimes passaram a envolver também o furto de criptoativos (DNI, 2024, p. 22). Segundo relatório da empresa Chainalysis (2024), foram furtados US$ 2,2 bilhões de plataformas de criptoativos, sendo que destas, US$ 1,34 bilhões estão relacionados a 47 ações executadas por atores norte-coreanos em 2024. Em 2023 foram US$ 660,50 milhões obtidos em 20 ações (CHAINALYSIS, 2024). Percebe-se que são valores significativos. A explicação detalhada do furto ocorrido na Coinspaid, que foi semelhante ao do Atomic Wallet, está disponível em Kuzin e Krupyushev (2023).

O relatório do Painel de Peritos da ONU de 7 de março 2024 informa que estavam investigando 58 ataques cibernéticos suspeitos, ocorridos entre 2017 e 2023, os quais teriam desviado valores de aproximadamente US$ 3 bilhões para o governo norte-coreano (ONU, 2024a, p. 60). No Anexo 59 do mesmo relatório foi elaborada uma lista não-exaustiva de 85 casos de interesse de ações executadas por grupos associados à Coreia do Norte no ano de 2023 (ONU, 2024a, pp. 319-332).

Por fim, considerando os gastos estimados do país com o desenvolvimento de armas nucleares (US$ 853 milhões) (ICAN, 2024, p. 15), só as ações ofensivas ilícitas relacionadas aos criptoativos já seriam suficientes para sustentar este projeto.

5.2.3 Outras ocorrências

Em 2014 outro caso chamou bastante a atenção: a invasão aos sistemas da empresa estatal sul-coreana *Korea Hydro and Nuclear Power Company* (KHNP), a qual administra usinas nucleares e hidrelétricas do país. Em dezembro daquele ano, a empresa teve seus sistemas comprometidos e plantas dos seus reatores nucleares, vazadas. O atacante se denominava "presidente do grupo anti-reator nuclear" e se declarava contra o uso de energia nuclear. Fazia ameaças dizendo que, se três dos reatores não fossem desligados até o Natal daquele ano, as pessoas deveriam distanciar-se de qualquer um deles. A usina possuía 23 reatores e fornecia aproximadamente 35% da energia consumida pelo país.[168] Provavelmente o ataque foi executado por meio da técnica de *spearphishing*, com arquivos manipulados para explorar a falha de um programa utilizado na empresa. Depois instalaram uma *backdoor*, obtiveram os arquivos e, em seguida, apagaram todos os dados dos dispositivos de armazenamento das máquinas, usando um *wiper* com código similar ao usado no *Sony Hack*. Ao final, a ameaça restou vazia, mas motivou mudanças nas políticas de segurança cibernética da Coreia do Sul. O governo sul-coreano atribuiu, em nota, a ação ao APT Kimsuky, o mesmo que perpetrou o ataque Dark Seul em 2013, e ao estado norte-coreano (STAHLER, HAGGARD, 2015; LEE, 2024). A semelhança de código do *wiper* utilizado nesse caso e no da Sony sugere a troca de conhecimento existente entre os grupos Lazarus e Kimsuky. Invasões a sistemas de usinas nucleares e empresa atribuídos ao Kimsuky continuam ocorrendo (SEUNG-WOO, 2021).

Existem situações, envolvendo partes do espaço cibernético, que a Coreia do Norte usa, conforme relatórios, de forma irregular. Uma delas é a adulteração da identidade digital[169] (número IMO) de navios, utilizada nos *Automatic Identification System* (AIS) *transponders*. Estes equipamentos são transmissores e receptores de ondas eletromagnéticas, através das quais as informações são compartilhadas permitindo, dentre outras funções, o monitoramento de embarcações e de sua posição. A falsificação de dados das mensagens AIS é utilizada pela Coreia do Norte para mascarar o uso de navios sancionados pelo Conselho de Segurança da ONU, enquanto executam ações ilícitas, como a transferência entre navios de material, também

[168] Atualmente a empresa ainda é a maior geradora de energia do país. Em 2023, forneceu 31,56% da energia consumida pelo país. Segundo dados de junho de 2023, 82,80% da energia daquele mês foi gerada por 27 reatores nucleares distribuídos entre suas 8 usinas nucleares.

[169] A identidade digital de uma embarcação é um número de sete dígitos dado pela agência da ONU para assuntos marítimos, a Organização Marítima Internacional (IMO, do inglês *International Maritime Organization*), que a acompanha desde sua fabricação, até o fim de sua vida operacional (C4ADS, 2021, p. 4).

sancionado, seja para exportação ou importação, de forma que não possam ser encontrados e abordados (C4ADS, 2021, ONU, 2024a).

Nos últimos anos trabalhadores norte-coreanos têm se infiltrado em empresas de TI, atendendo a ofertas de emprego. Como a demanda é grande e o país tem pessoal capacitado, eles candidatam-se às vagas, seja para trabalho efetivo ou *freelancer*. O objetivo final é ter acesso à rede corporativa da firma contratante e invadir seus servidores. Chegaram também a criar empresas nos EUA que intermediam o processo entre a firma e o empregado que, claro, não se apresenta como um cidadão norte-coreano, mas sob outra identidade. Segundo levantamento do Departamento de Justiça dos EUA, o pagamento dos trabalhadores, no fim, seria direcionado ao Ministério da Defesa norte-coreano ou a agências relacionadas ao desenvolvimento de ADM (TURTON, 2024; EUA, 2023a; SAKALLARIADIS, 2023; EUA, 2023b, p. 22; ONU, 2024a; WHITE, 2022; WHITE, 2024).

Outro caso recente e engenhoso foi a manipulação da *blockchain* Ronin bridge, usada pelo jogo Axie Infinity da empresa Sky Mavis. Nesta cadeia ficavam registradas transações ocorridas entre jogadores como, por exemplo, a venda de acessórios ou armas de personagens, utilizando a criptomoeda Ethereum. Esta ação rendeu US$ 625 milhões para o país. Para lavar esse dinheiro, utilizaram até agosto de 2022 a plataforma Tornado Cash, que já era sancionada pelo OFAC do Departamento do Tesouro dos EUA, mas permanece no ar. O esquema foi bastante inovador e mostra que o país tem buscado mudar suas técnicas e utilizar tecnologias novas (ONU, 2024a; TRMLABS, 2023; WHITE, 2024).

Bruce *et al.* (2024) publicaram um estudo a partir de um *suvey* enviado para especialistas em crimes cibernéticos, entre março e outubro de 2021. Como resultado da pesquisa, propuseram e calcularam um índice denominado WCI (*World Cybercrime Index*), que mediria a criminalidade cibernética (ou "cibercriminalidade") dos países. O índice categorizou as questões em cinco tipos de crimes, todos relacionados de alguma forma a ganhos financeiros. A Coreia do Norte ficou na sétima posição, segundo o cálculo, indicando que a percepção dos respondentes, se trata do sétimo que mais hospedaria criminosos cibernéticos.

Se tais crimes parecem, às vezes, distantes da realidade do Brasil, chamo a atenção para um caso de lavagem de dinheiro possivelmente proveniente de furtos de criptoativos pelo grupo Lazarus, em 24 de junho de 2022, segundo investigações do FBI (FBI, 2023). Parte desse dinheiro estaria sendo lavado por um cidadão russo, preso na Argentina, que operava por meio da corretora de criptoativos Binance e mudava de endereço constantemente. Além da Coreia do Norte, também prestaria esse serviço para comerciantes de pornografia infantojuvenil e terroristas (DI NICOLA, 2024; PAGANINI, 2024). Uma fonte citava a possibilidade de dois

cidadãos brasileiros estarem, também, envolvidos na lavagem de dinheiro, mas não foi possível confirmar isso com outras fontes abertas (CISO Advisor, 2024b). Como se pode imaginar, entretanto, essa mudança constante de domicílio pode, eventualmente, levar criminosos envolvidos em ações similares a vir para nosso país. Recentemente um relatório do Departamento do Tesouro dos EUA demonstrou uma rede de empresas e pessoas envolvidas na lavagem desse dinheiro usado, segundo afirmado, no financiamento dos programas de mísseis e armas de destruição em massa do país asiático (EUA, 2024a).

5.3 Cooperação em atividades cibernéticas

Dentro de teorias realistas, como o realismo estrutural (ou neorrealismo) de Waltz, um estado pode ter diversos objetivos, mas primeiramente ele tem a necessidade de sobreviver dentro da anarquia do Sistema Internacional. Assim que sua sobrevivência é garantida, ele pode buscar outros objetivos (WALTZ, 1979, pp. 91-92, 126). No caso da Coreia do Norte, não é diferente. O espaço cibernético não tem uma componente geográfica que permita a formação de alianças regionais, como a OTAN, Mercosul ou a União Africana. Ainda assim, no âmbito dessas alianças há trocas de informações sobre defesa cibernética (às vezes também envolvendo a segurança cibernética). Os países componentes da OTAN, por exemplo, formaram um centro militar de excelência sobre o assunto, o *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), cuja missão é "apoiar os nossos países membros e a OTAN com conhecimentos interdisciplinares únicos no domínio da pesquisa, formação e exercícios de defesa cibernética, abrangendo as áreas foco de tecnologia, estratégia, operações e legislação"[170] (CCDCOE, 2024, n.p., tradução minha). Importante destacar que não faz de estrutura de comando ou de força da OTAN, nem é por ela diretamente patrocinado, mas sim por países que a compõem (SCHMITT, 2018, p. 1).

Para a China, integrar-se com a Coreia do Norte é importante porque a auxilia a manter a estabilidade do regime norte-coreano e, por consequência, de sua economia, de forma a evitar imigração em massa através da longa fronteira. Uma demonstração disso é a integração entre as cidades de Dandong e Sinuiju, as quais estão no limite oeste da fronteira entre os dois países, como se percebe no mapa da Figura 20. As cidades estão distantes 1 km, separadas pelo rio Yalu (como chamado pela China) ou Amrok e Amnok (como é conhecido na Coreia), unidas pela Ponte da Amizade Sino-Coreana (PACHECO-PARDO, 2013).

[170] Texto original: "Our mission is to support our member nations and NATO with unique interdisciplinary expertise in the field of cyber defence research, training, and exercises covering the focus areas of technology, strategies, operations, and law."

Figura 20 – Mapa recente da Coreia do Norte

Fonte: Wikimedia Commons, derivado de mapa pelas Nações Unidas.

É através dessa ponte que muito do comércio entre os países tem sido feito, tanto no mercado formal quanto informal, assim como a terceirização de alguns trabalhos, devido à mão de obra norte-coreana ser mais barata (PACHECO-PARDO, 2013).

O relatório de 2014 da empresa HP, já citado, mostra que, nessa época, a conectividade à Internet era prestada pela China Telecom, bem como o fornecimento dos equipamentos de rede necessários (HP, 2014, p. 42). Entretanto, conectividade à Internet não é colaboração nem aliança, é só o provimento de um meio físico e de enlace.

Já foi relatado que a China teve uma participação importante no início da capacitação norte-coreana nas suas ações, pois, em 1992, especialistas em computação foram treinados por aquele país e retornaram com a ideia de usar a Internet para furtar segredos e atacar inimigos do governo, afirmando que a China já estaria fazendo isso (YOON, 2011; SANGER, 2018, pp. 127-128; CORERA, 2015, p. 302). A cidade chinesa de Shenyang também teve, no início, importante papel, pois lá havia hotéis e restaurantes administrados por norte-coreanos e teria sido usada como base de ataques (SANGER, 2018, p. 128). Os militares, enquanto eram treinados, ficavam se hospedavam em estabelecimentos supostamente de propriedade mista sino-norte-coreana, de modo que houvesse algum monitoramento das suas atividades (CARLIN, 2018, p. 320). Como até hoje a China é uma das bases utilizadas para ataques (tanto por acesso remoto, quanto para operadores lá residentes, diz-se que o país é complacente com as atividades e não desejaria resolver tal questão (KU, 2021, p. 269; PARK, PEARSON, 2017; O'NEILL, 2017). Não se trata de uma aliança formal, mas de um apoio significativo, ao prover estrutura física aos ataques e uma imunidade velada aos cidadãos daquele país, já que não haveria interesse em prendê-los e nem mesmo mitigar os ataques (KU, 2021, p. 270). Apesar dessa colaboração aparentemente velada, o levantamento feito por Izycki (2021, p. 68) cita registros documentados de ao menos sete ataques da Coreia do Norte contra alvos chineses. Dessa forma, entende-se não haver, atualmente, uma aliança formal voltada à troca de tecnologia entre os dois países.

Rússia, outra aliada de décadas (igualmente interessada em manter a Coreia do Norte servindo de *buffer* entre ela e a Coreia do Sul, onde há bases estadunidenses), teria transferido conhecimento e treinado *hackers* norte-coreanos há vários anos, inclusive com a contratação de 25 técnicos soviéticos, em 1986, para treinar seus militares (HP, 2014, p. 43; YOON, 2011; SANGER, 2018, p. 128; O'NEILL, 2017). Curiosamente, a Rússia foi um dos países mais afetados pelo *WannaCry*. Na época, o país não deveria ter muita preocupação com sua segurança cibernética, dado que o ataque afetou inclusive o banco central russo (KOTTASOVÁ, 2017). Cabe dizer que a Rússia, hoje, é uma potência no campo cibernético, com diversos grupos governamentais executando ações contra vários países (EUA, 2024b; HÖNÖ, 2023). Cumpre dizer também que o Brasil tem sido alvo de ataques, inclusive de espionagem, de grupos russos (DENESSEN, 2024).

A Síria é aliada da Coreia do Norte há tempos, recebendo cargas de armas e munições na década de 1960 e mantendo um acordo de cooperação militar e tecnológica assinado desde 1990 (BAR-ZOHAR, MISHAL, 2012, p. 280; ONU, 2018, pp. 48-53; ONU, 2018, pp. 41-43; BUREAU 39, 2020), inclusive envolvendo equipamentos de proteção, armas químicas e biológicas (KASZETA, 2021, p. 212; LEVKOWITZ, 2017; BERMUDEZ, Jr., 2013). Os sírios chegaram a iniciar, secretamente, a construção, com financiamento iraniano, de uma instalação nuclear, numa localidade denominada Al-Kibar, próximo à cidade de Dir Al-Zur[171], perto da fronteira com a Turquia. A obra contava com pessoal, tecnologia e equipamentos norte-coreanos e tinha, inclusive, a mesma estrutura da usina de Yongbyon (BAR-ZOHAR, MISHAL, 2012, pp. 280-282; DNI, 2008, pp. 3-5). Informações de Inteligência dos EUA afirmam que o objetivo norte-coreano nessa construção seria a obtenção de dinheiro, não combustível nuclear (DNI, 2008, pp. 12-13). No dia 6 de setembro de 2007, logo depois da meia-noite, caças israelenses invadiram o espaço aéreo sírio, bombardearam o local da construção e retornaram a Israel, ação batizada como Operação Pomar[172], com morte de trabalhadores norte-coreanos (BAR-ZOHAR e MISHAL, 2012, p. 280; ARI GROSS, 2018; MELMAN e RAVIV, 2018; SETH, 2020, p. 480; FOLLATH, STARK, 2009; LEVKOVITZ, 2017). Apesar de haver uma possibilidade de parcerias e cooperação em temas de segurança cibernética entre os países, não é algo que se tenha observado (RAMANI, 2021). Foi encontrada só uma referência à assinatura, em 2012, de um acordo para compartilhamento de informações envolvendo, dentre outros temas, TI (STEVENSON, 2012).

Com o Irã, a Coreia do Norte colabora no projeto de mísseis balísticos e em temas nucleares (LEVKOWITX, 2017, pp. 21-23). Ainda, há também cooperação com grupos terroristas associados ao Irã, como Hezbollah e Hamas, em temas como treinamento, troca de tecnologias, fornecimento de munições e possivelmente mísseis (LEVKOWITX, 2017). Um acordo assinado, em 2012, entre os países, envolveria transferência de tecnologia nas áreas de TI, energia, meio ambiente, agricultura e alimentação (HP, 2014, p. 44; AL JAZEERA, 2012). Possíveis evidências da cooperação entre os países são as semelhanças entre o ataque cibernético do tipo *wiper* executado pelo Irã, em 2012, contra a empresa saudita Saudi Aramco, denominado Shamoon, e o Dark Seul, executado pela Coreia do Norte, sete meses depois, contra alvos na Coreia do Sul (WHITE, 2022, cap. 4). O ataque norte-coreano poderia ser

[171] Outras grafias usadas para a região: Dair Alzour, Deir al-Zor, Deir Zor Deir ez-Zor, Deir Ezzor, Deir al-Zor, Dayr al-Zawr, Dayr az-Zawr, Der Ezzor, Deirazzor e Zor.

[172] Tradução de *Operation Orchard*, mas também denominada Fora da Caixa (*Outside the Box*) ou Melodia Silenciosa (*Silent Melody*).

somente um *copycat*[173] do ataque iraniano. Entretanto, como sugeriu um antigo diretor do *Government Communications Headquarters* (GCHQ), serviço de inteligência britânico responsável pelas áreas de inteligência, segurança e cibernética, é possível que tenha havido cooperação entre os países (SANGER, 2018, pp. 130-131).

Outros países que servem como base para ataques são a Malásia, incluindo a criação de supostas empresas *startup* de fachada e Singapura (PARK, PEARSON, 2017; O'NEILL, 2017). Entretanto, não se trata de cooperação, mas de uso irregular desses países citados. O mesmo pode ser dito de outros mencionados: Índia, Nova Zelândia, Nepal, Quênia, Moçambique e Indonésia.

Com relação à diplomacia digital, não foram encontrados registros da presença ostensiva norte-coreana em palcos de discussões diplomáticas sobre temas digitais e governanças. Ao contrário, o país permanece sancionado devido à sua atuação, como relatado. Também não aparenta usar ferramentas inovadoras na prática diplomática, exceto por meio de sítios oficiais (ministérios e embaixadas) e do seu portal Naenara, onde disponibilizam informações a usuários, praticamente em usos similares como os vistos na Web 1.0 (O'REILLY, 2005; CORMODE, KRISHNAMURTI, 2008).

No que tange à diplomacia cibernética, o país surpreendeu ao ser um dos vinte propositores, em 2019, de uma convenção das Nações Unidas para combate a crimes cibernéticos. Com o texto aprovado pela Assembleia Geral em setembro de 2024, resta ver qual será a atuação do país diante de casos que envolvam seus cidadãos, ou mesmo sua própria estrutura militar. Entretanto, não apresenta equipe de CERT ou CSIRT ativa que possa ser contactada nas situações de incidentes de segurança cibernética (que incluem os crimes cibernéticos). A Coreia do Norte também não participa da Interpol nem demonstrou interesse na Convenção de Crimes Cibernéticos (Convenção de Budapeste).

5.4 Coreia do Norte como alvo de ataques cibernéticos

Apesar de sua estrutura cibernética *militar* ser supostamente melhor que de alguns países desenvolvidos, em 2022 o país foi alvo de um ataque cibernético como os imaginados na década de 80 e 90: aquele *hacker*, normalmente estereotipado como um adolescente morando no porão da casa dos pais, executa um ataque capaz de penetrar qualquer sistema, inclusive de potências nucleares, causando uma guerra nuclear. No filme Jogos de Guerra (título original: *WarGames*), de 1983, durante a Guerra Fria, um *hacker* secundarista invade o sistema de

[173] Usa-se o termo *copycat* quando algum ataque parece ser exatamente uma imitação de outro.

controle automatizado de lançamento de armas estratégicas e executa ações que sugerem ao sistema dos Estados Unidos estarem sendo atacados por armas nucleares soviéticas. No caso do filme, a invasão acontece por acaso e não havia intento pelo "atacante" de executar qualquer ação contra o inimigo. A propósito, ele não acreditava que haveria um inimigo real, mas que se trataria de um jogo de simulação (JOGOS [...], 1983).

O *hacker* Alejandro Caceres (ou P4x, como foi escolheu ser chamado), ao contrário de David Lightman (nome do personagem interpretado por Matthew Broderick no filme citado), sabia quem era o alvo, conhecia exatamente que partes da infraestrutura cibernética atacava e, além disso, tinha uma motivação. No caso, vingança por ter sido alvo de ataques daqueles que atacava. E não seria um secundarista, mas um pesquisador da área de segurança cibernética. P4x teria sido um dos alvos em uma operação por supostos espiões norte-coreanos. Tal operação objetivava atingir pesquisadores da área de segurança cibernética para adquirir suas ferramentas de trabalho (ou talvez seriam armas cibernéticas?) e compor o kit de ataque norte-coreano. P4x, com a percepção de que o Estado não fez nada com as informações que repassou, resolveu tomar as rédeas da ação e retaliou o estado norte-coreano com ataques de negação de serviço a servidores e roteadores (GREENBERG, 2024; GREENBERG, 2022; NEWMAN, 2021; SMITH, 2022).

Como curiosidade, houve um alerta, em 1994, conforme relatado, de que alguém, após invadir redes militares dos EUA, supostamente estaria tentando, a partir destas, acessar a rede de uma instalação nuclear norte-coreana. O fato de isso ter acontecido durante uma negociação que ocorria entre EUA e Coreia do Norte, justamente a respeito de armas nucleares, levantou a suspeita de que tal tentativa fosse uma ação do governo que acabaria com a possibilidade de qualquer acordo. Ao final, esclareceu-se que a tentativa de acesso era a uma instalação sul-coreana (UNGOED-THOMAS, 1998; CORERA, 2015, pp. 164-167).

Poucos dias depois do ataque à Sony, a Internet ficou instável na Coreia do Norte dia 19 de dezembro de 2014 (sexta-feira), piorando no final de semana até que na segunda, dia 22, ficou completamente indisponível por dez horas. Na época hipóteses foram levantadas, inclusive retaliação dos EUA, já que no dia 19 o presidente Obama acusou diretamente o regime norte-coreano dos ataques à Sony (PERLROTH, SANGER, 2014).

Como já falado anteriormente, a princípio haveria, em 2016, somente 28 sítios de Internet no país (FRANCESCHI-BICCHIERAI, 2016b). Ainda que esse número seja baixo, o que claramente diminui sua superfície de ataque, há relatos de invasões sem muita relevância, como ao clone do Facebook (FRANCESCHI-BICCHIERAI, 2016a). O tamanho diminuto também permite que ataques, como o perpetrado por P4x, já descrito, tenham um grande

alcance, agravado pelo fato de não haver resiliência na rede naquela época. Também torna fáceis ações de espionagem, já que possui pouco mais de mil endereços IP alocados às suas empresas (WHITE, 2020, p. 71).

Depois do já bastante estudado ataque do projeto Olympic Games, mais conhecido pelo nome Stuxnet, executado pelos Estados Unidos e Israel contra as instalações nucleares de Natanz do Irã, em 2010, danificando centrífugas e atrasando em alguns anos o projeto nuclear deste país (ZETTER, 2014; WHITE, 2020, pp. 220-246), os mesmos Estados Unidos teriam tentado atacar a Coreia do Norte de forma similar, não obtendo o mesmo sucesso (MENN, 2015). Entretanto, documentos vazados em 2017, durante o governo de Barack Obama, indicam que ataques cibernéticos de sabotagem foram executados contra o programa de mísseis norte-coreano. Esses ataques executaram o que é chamado de "*left of launch*"[174], o que normalmente consiste em usar tecnologias que desabilitam mísseis antes da chegada ao local de lançamento ou assim que são lançados. Alguns lançamentos teriam sido bem sucedidos, enquanto outros apresentaram problemas, o que pode sugerir o sucesso de tais ataques (SANGER, BROAD, 2017).

Não há surpresa ao se verificar que ambos os ataques relatados, executados pelos Estados Unidos, teriam como objetivo final não a estrutura cibernética da Coreia do Norte, mas sim projetos militares que ofereçam risco àquele. A própria Coreia do Sul também já publicizou que estaria desenvolvendo armas cibernéticas ofensivas com o objetivo de atacar as estruturas e armas nucleares do seu vizinho (KECK, 2014). Tentativas recentes de lançamentos de satélites espiões pela Coreia do Norte foram fracassadas, o que pode estar relacionado a ações cibernéticas ou a uma nova tecnologia de propelente que estava sendo usado pela primeira vez (KIM, KIM, 2023; XU, 2024).

Recentemente, um servidor de arquivos aberto (sem proteção por senha) foi descoberto na Internet da Coreia do Norte. O tráfego do servidor e o conteúdo nele armazenado foram estudados por pesquisadores e uma empresa de segurança cibernética, sendo identificado que o equipamento servia para troca de arquivos relacionados a projetos de animação. Empresas de fora da Coreia do Norte enviavam arquivos e orientações para empresas ou pessoas norte-coreanas subcontratadas para trabalhar nesses projetos. Tais projetos, aparentemente, seriam de oriundos de companhias dos EUA, China, Japão e Reino Unido que, não necessariamente, teriam conhecimento do uso de mão de obra norte-coreana por outra empresa que teriam contratado (WILLIAMS, 2024b).

[174] Numa tradução livre: "cessar o lançamento".

A Coreia do Norte está numa situação vantajosa comparada ao resto do mundo em relação a um item: sua superfície de ataque é bastante limitada. Sua infraestrutura seria tão defasada e, o país tão desconectado, que se torna praticamente invulnerável a ataques cibernéticos. A ausência de redes de comunicação e uma sociedade que não as acessa podem ser pensadas como algo negativo, mas há o benefício de limitar as possibilidades de ataque para seus inimigos. Em ataques cibernéticos por vezes é necessário transferir arquivos com conteúdo malicioso e ataques de engenharia social necessitam que pessoas sejam convencidas a executar ações determinadas pelo operador do ataque. O isolamento da população em uma rede à parte da Internet a protege e aos demais dispositivos e indivíduos ali conectados, permitindo que o país possa empreender ações cibernéticas ofensivas sem grandes riscos de retaliações nessa seara. Assim, o atraso da Coreia do Norte quanto ao uso e à popularização de tecnologias acaba se mostrando uma vantagem, em termos de segurança, diminuindo sobremaneira a suscetibilidade a esse tipo de ataque (HARRIS, 2015, p. 71).

Ainda assim, ataques ofensivos são possíveis. Buchanan (2020, pp. 124-125) comenta que em certa época a NSA pouquíssima informação quanto à Coreia do Norte. Entretanto, a Coreia do Sul tinha conseguido penetrar nas redes norte-coreanas. Dessa forma, a NSA invadiu a base de espionagem da Coreia do Sul, coletando os dados de inteligência que estes tinha coletado. Dentre as informações obtidas da Coreia do Sul estavam as informações de como invadir as redes do outro país e, depois de algum tempo, a própria NSA também penetrou as redes norte-coreanas posteriormente.

6 CONSIDERAÇÕES FINAIS

Um russo que trabalhou na URSS na época da Guerra Fria disse a William Langewiesche: “Se um país tomar a decisão política de tornar-se um Estado nuclearmente armado, ele conseguirá fazê-lo, apesar das sanções ou dos incentivos internacionais. Não é preciso ser rico. Nem necessariamente ser tecnicamente desenvolvido. Pode ser o Paquistão, a Líbia, a Coreia do Norte, o Irã” (LANGEWIESCHE, 2007, p. 21).

A Coreia do Norte há anos desenvolve armas nucleares, bem como vetores de lançamento. Atualmente tem demonstrado que sua “espada de múltiplos propósitos” conta com significativo ferramental de armas cibernéticas, que tem sido destaque nos palcos especializados, e até na ONU. Chris Inglis, ex-vice-diretor da NSA, reconheceu, em 2021, a sofisticação e aplicação do espaço cibernético para a Coreia do Norte na busca por (e alcance de) seus objetivos, com um baixo custo (PERLROTH, 2021, p. 335).

Em *Three Dangerous Men*, Seth (2021) avaliou o uso da guerra assimétrica contra os EUA, considerando os seguintes países como suas ameaças: Rússia, China e Irã. A Coreia do Norte foi deixada de fora pelo autor, cuja avaliação é a de que, apesar de o país ter capacidades cibernéticas, mísseis e armas nucleares, faltaria uma maior economia para, nas palavras dele, ter alguma projeção de poder e se juntar aos outros três. Dessa forma, no título consta *Three*, e não *Four.* Apesar dessa falta de projeção de poder, suas capacidades cibernéticas, na verdade, “projetam” perigos a vários outros países, sem que haja uma perspectiva de mudança. Domingo (2025, p. 266), no entanto, considera como sendo atores relevantes no espaço cibernético as três grandes potências (Rússia, China, EUA), acrescidos de Irã e Coreia do Norte, devido ao engajamento ativo que os dois últimos têm demonstrado. Kello (2019, p. 152) também entende que a Coreia do Norte, com a criação do *Bureau 121*, deu o primeiro passo para, hoje, ser considerada o que ele chamou de “potência cibernética”.

Considerando a evolução alcançada pelo país, e o que foi apresentado por este estudo, a seguir respondo às questões norteadoras da pesquisa, que buscou sobretudo descrever e analisar como a Coreia do Norte atua no espaço cibernético, no que tange a crimes.

A avaliação de quais seriam os objetivos das suas atividades cibernéticas ofensivas, mostra que as atividades de espionagem são as mais presentes, conforme análises executadas por empresas especializadas e relatórios de agências nacionais de inteligência. Além destas, há diversas ações ofensivas para obtenção de divisas. Os valores daí advindos são direcionados para o financiamento do regime e, principalmente, para a continuação do desenvolvimento de armas de destruição em massa, como armas nucleares, e da tecnologia dos vetores de entrega

das mesmas (mísseis). Tais armas permanecem como uma peça importante no contexto da política mundial na balança de poder.

Recentemente percebeu-se uma inovação nas ações no espaço cibernético, envolvendo o furto de carteiras digitais de criptoativos de corretoras e de jogos virtuais que utilizam as mesmas tecnologias. Comparando os valores obtidos nesses furtos e o custo anual do programa nuclear norte-coreano, percebe-se que ele pode ser sustentado apenas pelas ações cibernéticas.

A pesquisa mostrou também que o desenvolvimento das suas capacidades cibernéticas acontece internamente, ou seja, por meio da capacitação de pessoas, as quais costumam ser selecionadas a partir da identificação de talentos ainda na escola, sendo direcionadas para universidades técnicas do país e contratadas para executar as atividades em seu nome, sempre com algum tipo de conexão com as Forças Armadas como, por exemplo, o *Bureau 121*. O país também obtém conhecimento a partir do furto de ferramenta de outros atores, como evidenciado nos relatórios dos *experts* de empresas de segurança cibernética ou de governos. O senso comum pode até apontar para outra direção, mas o país desenvolve, há anos, sua infraestrutura voltada para o espaço cibernético, contando com mão de obra especializada que, ao que tudo indica, é bastante capacitada.

Quanto a alianças de cooperação com outros países, o estudo demonstra que há tratados assinados, mas não foi possível identificar qual o tipo e nível de troca de conhecimento que eles implicam. A troca, entretanto, existe, como pode ser visto a partir da semelhança entre TTP de ações executadas por iranianos e norte-coreanos (como as operações Shamoon e Dark Seul, por exemplo).

No que se refere à Coreia do Norte como vítima de ataques, considerando que o país também é um alvo de ações cibernéticas por outros, ficou evidente que ele apresenta uma superfície de ataque limitada, ou seja, a sua baixa conectividade à Internet, as formas bastante limitadas de acesso à conectividade, além da opacidade da estrutura governamental protegem o país de ameaças cibernéticas externas. Entretanto, ainda assim há algumas possibilidades, as quais já foram exploradas pela agência de inteligência da Coreia do Sul e pela NSA dos EUA, por exemplo.

Por fim, não se perceberam incentivos para que o país deixe de praticar tais ações. Sanções econômicas têm surtido efeito limitado, por alguns motivos: nem todos os países implementam as sanções que buscam coibir suas atividades e, mesmo dentre os que implementam, nem todos as tem aplicado, além do que a Coreia do Norte tem aprendido formas para burlar essas sanções, o que normalmente ocorre mediante o uso de tecnologias que são desenvolvidas e utilizadas amplamente pelos seus adversários. Cabe ainda destacar que há um

vácuo nas legislações internacionais que impede uma atuação mais ampla de outros países contra os atores cibernéticos norte-coreanos.

6.1 Limitações da pesquisa

O tema estudado, principalmente por envolver questões de segurança e defesa nacional, não oferece, por vezes, fontes de informação abertas e disponíveis para o público em geral. Entretanto, o uso de fontes abertas sem a correta identificação quanto à sua qualidade abre oportunidades para que informações e desinformação sejam difundidas. Tomou-se o cuidado de selecionar as fontes de maneira criteriosa para que isso não ocorra.

Além disso, trata-se de uma área de pesquisa de assunto contemporâneo sobre o qual, a cada dia, surgem novas informações quanto a vulnerabilidades em sistemas computacionais, execução de novos ataques e até atribuições a ataques anteriores que eram desconhecidas.

A distância temporal de eventos ajuda a analisar melhor os fatos em certas situações. No caso de algumas questões aqui estudadas, o fato de uma guerra estar ocorrendo, com envolvimento direto da Coreia do Norte no conflito, prejudica a construção de algumas conclusões como, por exemplo, qual o impacto do tratado de cooperação assinado no segundo semestre de 2024 entre os norte-coreanos e russos. O mesmo pode ser dito da recém assinada convenção da ONU voltada para crimes cibernéticos, igualmente assinada no segundo semestre de 2024, cujos impactos ainda estão longe de ser conhecidos.

Por fim, mas não menos importante, há a limitação linguística do autor. Para quem não é leitor de coreano, documentos oficiais vazados do governo norte-coreano, publicados pelo governo da Coreia do Sul, ou de pesquisadores deste país, acabaram por não ser considerados neste trabalho, quando não tinham tradução, por exemplo, para o inglês. Entretanto, tomou-se o cuidado de se utilizarem documentos mais técnicos e sítios da Internet, além de pesquisas e livros acadêmicos de fontes variadas. Foram consultadas fontes estadunidenses e europeias sobre o tema, principalmente, no intuito de suprir lacunas relativas a um país tão opaco e isolado, cujo idioma não é tão simples para falantes do português.

6.2 Implicações práticas

Trago, nesta seção, algumas implicações práticas e discussões desse estudo para atores internacionais selecionados (países e organizações), considerando tanto questões relativas à segurança cibernética de modo mais amplo, quanto envolvendo relações com a Coreia do Norte mais especificamente.

Kan *et al.* de 2010 (p. 28) afirmaram, já há algum tempo, que a Coreia do Norte continuaria a praticar o que chamaram de *soberania criminal*, principalmente por meio das ações engendradas pelo *Bureau 39*, tendo como objetivo a sobrevivência do regime e o seu progresso militar. Os autores ainda apresentaram a evolução de tais atividades conforme o passar dos anos, prevendo que a evolução persistiria. Depois de mais de uma década da publicação do artigo, sua conclusão se sustentou: o país progrediu nas suas ações criminosas, principalmente, passando a utilizar atividades cibernéticas ofensivas, as quais não são mais executadas pelo *Bureau 39* do Partido dos Trabalhadores Coreanos, mas pelo *Bureau 121* do *Reconnaissance General Bureau* (RGB), órgão estatal de operações clandestinas. Ao que parece, principalmente por documentários recentes, o *Bureau* 39 permanece ativo, atuando também de forma clandestina para obter novas formas de financiamento ou, segundo outras fontes, cuidando somente de valores desviados para sustentar os luxos da família Kim.

Para a Coreia do Sul, a ameaça cibernética imposta pelo país vizinho não deve ser negligenciada, já que consiste no principal alvo dos ataques norte-coreanos conforme alguns estudos (IZYCKI, 2021, p. 58), ou o segundo, de acordo com outros (MICROSOFT, 2022; MICROSOFT 2023). Para diminuir tal ameaça, Ku (2021, p. 274) lembra que muitos dos ataques executados pela Coreia do Norte são feitos a partir de bases fora do país, de modo que sanções impostas a Pyongyang seriam ineficazes, principalmente porque envolvem a China (KU, 2021, p. 269). O autor sugere, então, analisando a Estratégia Nacional de Segurança Cibernética sul-coreana, que a Coreia do Sul deveria sinalizar a inadequação desse comportamento dentro de sua política de segurança cibernética nacional. Ao mesmo tempo, sugere estabelecer parcerias com nações com posturas similares, citando os chamados *Five Eyes* (Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia), junto com Japão, Alemanha e França (KU, 2021, p. 274). Na mesma direção, Platte (2021) afirma que se deve criar uma estratégia de dissuasão cibernética pelo país, para unir ou fortalecer alianças com parceiros, como fizeram os membros integrantes da OTAN. A Coreia do Sul precisa considerar em suas políticas de defesa, especialmente, a proteção à sua infraestrutura crítica

Para os EUA, a Coreia do Norte permanece uma ameaça também no espaço cibernético. Ataques de inteligência para furto de propriedade intelectual, por exemplo, e a bancos para furto de valores já foram identificados e alguns, mitigados. Já houve ataques a infraestruturas críticas, mas sem relatos de sucesso. As Estratégias Cibernéticas Nacionais de 2018 e 2023 citam a Coreia do Norte como um adversário a ser observado. A CISA e o FBI já emitiram diversos documentos tratando especificamente de ameaças norte-coreanas, como o I-051624-PSA emitido em 16 de maio de 2024 (FBI, 2024b) e o I-090324-PSA, de 3 de setembro de 2024

(FBI, 2024c). A CISA também possui uma página em seu sítio da Internet na qual apresenta, no contexto de suas atribuições, informações acerca da ameaça que a Coreia do Norte representa e com ligações para documentos de recomendações[175]. Há páginas semelhantes para outros países adversários, China, Rússia e Irã.

No que concorre a nós, o Brasil tem evoluído nos últimos anos na área de segurança cibernética, com a elaboração de leis desde o Marco Civil da Internet, em 2014. Mais recentemente o país publicou a Estratégia Nacional de Segurança Cibernética (e-Ciber), criou a Autoridade Nacional de Proteção de Dados (ANPD), além do Comitê Nacional de Cibersegurança (CNCiber). A Agência Nacional de Cibersegurança (ANCiber), entretanto, ainda se encontra pendente de aprovação pelo legislativo. Não à toa somos bem classificados em índices como o elaborado pela ITU: em 2024 o país ocupou a primeira faixa (T1) dos países referências, com índices acima de 95 em 100 (ITU, 2024).

Ainda assim, o Brasil é alvo de ataques cibernéticos pela Coreia do Norte, principalmente para obtenção de informações (espionagem) e, possivelmente, continuará sendo. Contudo, sua preocupação na elaboração de leis, criação de agências e participação em órgãos multilaterais no combate a crimes cibernéticos e difusão de conhecimento é algo digno de nota. Importante ressaltar a participação ativa que o país tem com representantes em diretorias da Interpol.

Sobre as relações diplomáticas entre o Brasil e a Coreia do Norte, elas têm se mantido e não há indicativos que estejam ameaçadas. A posição brasileira é favorável nos diálogos, dentre outras razões, por não possuir nenhum interesse securitário na situação da península (SIEBRA, 2017, p. 225). Considerando os bons relacionamentos entre a DPRK, Rússia e China, países que fundaram o grupo BRICS junto com o Brasil, é possível dizer que este grupo também seria um fórum possível de comunicação e facilitação de negócios, atendendo aos nossos interesses nacionais. Entretanto, é sempre bom lembrar que os três países executam recorrentemente ataques cibernéticos direcionados ao Brasil ou empresas brasileiras (DENNESEN *et al.*, 2024) e contra isso nós devemos, continuamente, nos proteger.

Quanto a organismos internacionais, o Conselho de Segurança da ONU já emitiu sanções de diversos tipos à Coreia do Norte. Entretanto, há países que não seguem tais sanções, incluindo a China, com quem existem ligações econômicas e compartilhamento de uma extensa fronteira, e a Rússia, com quem recentemente foram firmadas compras de armamentos, no contexto da Guerra na Ucrânia, e foi firmado um acordo estratégico que inclui grande

[175] Disponível em: https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea. Acesso em: 21 jan. 2025.

cooperação militar e formas de comércio que burlam as sanções econômicas. Ainda, faz pouco tempo a Rússia vetou a continuação do Painel de Peritos referente à Resolução 1874 (ARNOLD, 2024), o qual, dentre outras atividades, fiscalizava e reavaliava o cumprimento das sanções determinadas pelo conselho. Este painel, desde 2018, levantou fatos sobre o uso de ações cibernéticas pela Coreia do Norte, primeiramente para espionagem e, em seguida, como forma de evitar as fiscalizações e sanções.

A Agência da União Europeia para a Cibersegurança (ENISA), em seu relatório mais recente, avaliou tendências de ameaças cibernéticas por atores associados à Coreia do Norte e orientou algumas ações para a segurança dos países e empresas (ENISA, 2024).

Quanto a acordos multilaterais relacionados a crimes cibernéticos, destaco que a Coreia do Norte não é (e não aparenta ter) interesse em participar da Convenção sobre o Crime Cibernético (Convenção de Budapeste). Entretanto, foi um dos países propositores da Convenção das Nações Unidas contra o Crime Cibernético, recentemente aprovada. Resta saber qual o real interesse do país com essa iniciativa, dado que a assinatura ainda ocorrerá neste ano de 2025. Além disso, cabe pensar como serão tratados os casos concretos, quando acusados de crimes forem seus cidadãos, ou evidências digitais precisem ser obtidas em suas redes de comunicação. Lembro também que o país nega ter um CSIRT estruturado, para colaborar em casos de segurança cibernética envolvendo sua rede.

A Coreia do Norte não se interessa em ser membro da Interpol e, por isso, este organismo não tem como atuar intermediando auxílios em investigação de crimes cibernéticos relacionados com aquele país. Ainda, caso fosse um país-membro, a organização não interviria em certas investigações que envolvessem seus militares ou questões políticas entre países, seguindo a regra de neutralidade imposta pelo artigo 3º da sua Constituição (INTERPOL, 2023; INTERPOL, 2006).

O relatório de 2017, da empresa Recorded Future, confirma que a Coreia do Norte age no espaço cibernético de forma bastante racional, conforme seus objetivos. Em sua análise, o país dá aos seus órgãos de inteligência um escopo mais abrangente, e seus atores cibernéticos, normalmente localizados dentro do *Reconnaissance General Bureau* (RGB), atuam de acordo com tal diretriz (RECORDED FUTURE, 2017).

A forma encontrada para tentar mitigar tais ações ofensivas foi a aplicação de sanções, a qual não tem surtido efeito. Ainda, questiono se certas iniciativas propostas pelo Painel de Peritos da ONU seriam aplicáveis. Por exemplo, a sanção a um grupo criminoso associado à Coreia do Norte que não pode ser facilmente identificado, como Lazarus, APT37, Kimsuky e ScarCruft. Esses nomes foram dados por empresas e ninguém sabe quem, efetivamente, são

seus componentes. No caso desse tipo de grupo abstrato, essa espécie de anonimato serve para atrelar diversas operações a ele, analisando vestígios durante a análise técnica, ou para correlacionar atividades que se utilizam da mesma carteira de criptoativos. Só que não se trata de estruturas oficiais de nenhum país, nem empresas com registro conhecido. Como Lin (2016, p. 85) comenta, a atribuição a uma pessoa, grupo de pessoas ou entidade organizacional é importante. Entretanto, entendo que ainda falta uma conexão com a realidade física que lhe serve como base. Destaco que outros países, como os EUA, já implementam sanções a tais grupos, ainda que, dado seu desconhecimento sobre quem o constitui, não tenham tido, pelo menos aparentemente, consequências concretas. Quando identificados, indivíduos são sancionados e processados pela Justiça do país, como foi o caso de um indivíduo norte-coreano, identificado como Jin Hyok Park, e de outros russos e chineses, principalmente.

6.3 Contribuições e trabalhos futuros

Na opinião de Kello (2017, p. 147), a posição da Coreia do Norte é única, pois "desafia, mas também reside, na medida em que pode, *fora* da sociedade anárquica de Estados"[176] (KELLO, 2017, p. 147, tradução minha, destaque no original). O país, com sua política de isolamento e autossuficiência, movida por um possível ressentimento por séculos de invasões, buscou proteger-se através do desenvolvimento das armas nucleares. Quando percebeu, no passado recente, que seus parceiros não teriam como apoiá-la financeiramente, buscou outras formas de obtenção de dinheiro, ainda que à luz da legislação de diversos países isso poderia significar a execução de crimes. Mais recentemente, como mostrou a pesquisa, o uso do espaço cibernético não só para ações de sabotagem e espionagem, mas também para furto de valores monetários, se transformou em uma nova ferramenta.

Como Kim Jong-il teria afirmado, as capacidades norte-coreanas no domínio do espaço cibernético seriam a *espada de múltiplos propósitos* compondo, com as armas nucleares e mísseis, a proteção e os recursos para ataques do exército nacional. No estudo atual, percebe-se que as ações cibernéticas são executadas para fins ofensivos de sabotagem, espionagem e obtenção de dinheiro.

Para Nye Jr. (2011) e sua definição de poder cibernético, bem como nos casos de uso (que ele chama de faces) desse poder não se incluíam a execução de ações cibernéticas ofensivas com ganhos financeiros. Afinal, depois dos piratas e corsários, obter dinheiro de forma ilegal não era mais uma atividade esperada de atores estatais (ou mesmo semiestatais) (EGLOFF,

[176] Texto original: "defies but also resides, insofar as it can *outside* the anarchical society of states."

2022). A Coreia do Norte subverteu, evoluindo suas capacidades cibernéticas, voltadas no início principalmente para ações de espionagem e sabotagem, para a obtenção de dinheiro, sem importar quem eram as vítimas, sejam bancos governamentais por meio de transações SWIFT fraudulentas, sejam pequenas empresas vítimas de ataques de *ransomware*, ou clientes de corretoras de criptoativos que tiveram suas carteiras levadas. Tal evolução aconteceu principalmente na última década e meia, com mudanças perceptíveis em suas táticas, técnicas e procedimentos a cada ano.

A subversão que trato, por sua vez, não se deve a esta evolução contínua. Ela foi importante. Deve-se principalmente ao fato de que, ao executar suas capacidades cibernéticas e obter dinheiro para o regime do país, esses valores direcionaram em gastos para os militares e desenvolvimento de armas de destruição em massa, fortalecendo seu poder militar. Poder militar que, no fim, aumentou sua relevância nos palcos internacionais, além de exercer dissuasão contra possíveis ataques de seus adversários.

Evitar o sucesso de ações cibernéticas ofensivas envolve soluções holísticas, que passam por estratégias e políticas de segurança cibernética nacionais, conscientização de empresas no desenvolvimento e uso de sistemas e configurações seguras, assim como de usuários. Isso minimiza a superfície de ataque a que os países estão sujeitos, no mínimo trazendo dificuldades para o atacante.

Uma forma de dissuasão e retaliação é a aplicação de sanções ao país, as quais poderiam supostamente infligir prejuízo econômico. Contudo, Visentini *et al.* (2018, p. 190) concluem, sobre as sanções à Coreia do Norte, que estas "não lograram qualquer dos seus objetivos, porque a economia não é globalizada." De fato, as sanções econômicas impostas pela ONU e outros estados, de forma unilateral, aparentam não ter efeito o efeito desejado e não têm sido suficientes – seja por falta de implementação, como o Painel de Peritos sugeriu em relatórios, seja porque outros países, inclusive do próprio Conselho de Segurança, têm ignorado e aproveitado, por exemplo, de mão de obra barata para suas empresas. Além disso, a Coreia do Norte tem conseguido burlar esses limites e se adequar usando inovações desenvolvidas pelos próprios países que são seus opositores, como o recente uso (e furto) de criptoativos.

Outras formas possíveis de conter sua atuação criminosa, como a assinatura de tratados e acordos internacionais, também não surtiram efeito. Quando assinados alguns, o país não exerceu o combinado, e, de outros, não demonstrou interesses em participar. No meu entendimento, a ausência do país na Interpol e a falta de um contato de auxílio como referência para situações que envolvam ocorrências de segurança cibernética, são indícios significativos da ausência de interesse em trabalhar de forma multilateral pela segurança neste domínio.

A aplicação de retaliações utilizando o mesmo tipo de ação, no domínio cibernético, seria uma possibilidade. Na prática, entretanto, não tem utilidade por diversos motivos, como a superfície de ataque mínima e o fato de que, ao executar um ataque ofensivo cibernético, o atacante permite que o alvo conheça suas TTP e, eventualmente, até consiga obter a ferramenta (código executável) utilizada. Ao contrário de um míssil que explode, ou de uma arma que dispara somente um projétil, uma ferramenta cibernética pode ser preservada e reutilizada. Ou então, por vezes, isso invalida a ferramenta por meio da correção da falha de segurança explorada.

A possibilidade explorada pelos EUA de identificar indivíduos específicos envolvidos nas ações e julgá-los nas cortes nacionais deve ter seu resultado avaliado. Ainda que o réu não cumpra a pena, expõe-se o país de forma indireta, visto que a investigação normalmente demonstra que eles trabalhariam para o Estado. Essa opção deve ser mais bem acompanhada em documentos posteriores.

Do ponto de vista da Coreia do Norte, a falta de uma alternativa que lhe ofereça a mesma segurança que a posse de tecnologia e armas nucleares, e que também lhe conceda relevância nos palcos internacionais, é motivo suficiente para continuar seguindo com seu desenvolvimento.

Como resultado, até agora, das ações cibernéticas que executou, o país conseguiu reposicionar de forma favorável a balança de poder no mundo de uma forma única. A construção da *espada de múltiplos propósitos*, idealizada por Kim Jong-il, não foi iniciada em 2014 com os ataques à Sony. Segundo os relatos apresentados, desde 1992 haveria uma ideia inicial, a partir de militares retornando da China, sobre as possibilidades de uso do espaço cibernético para atingir adversários. O início da capacitação de *guerreiros* cibernéticos aconteceria a partir de 1996, sendo formado o *Bureau 121* (ou alguma estrutura anterior) em 1998. Entretanto, tais informações não são certas. Ainda que se considere, o que entendo ser mais provável, a formação do *Bureau 121* no RGB a partir de 2013, o treinamento e estruturação de ações cibernéticas começou antes, provavelmente em outras estruturas do Exército ou no KWP, já que se tem conhecimento de algumas ações ofensivas desde ao menos 2009.

O fato é que, independentemente da data inicial, o custo financeiro para a estruturação de uma unidade de ações cibernéticas não é barato, pois inclui aquisição de equipamentos e, principalmente, capacitação de pessoal numa área extremamente especializada. Isso também não é executado rapidamente. Aliás, nem as próprias operações cibernéticas são executadas sem um planejamento anterior longo. Invadir e conhecer a rede do adversário, por vezes, exige-se anos de pesquisa até a execução completa do ataque, vide operações como a Red October (cinco

anos de execução, sem atribuição definida) e o assalto ao Banco de Bangladesh (acesso inicial em janeiro de 2015 com execução das transferências em fevereiro de 2016). São atividades demoradas que certamente exigiram muito tempo de pesquisa e dedicação dos seus executantes, o que também faz parte do custo da operação.

A construção de uma arma nuclear, mísseis e da estrutura necessária para lançá-los também é bastante cara. Ao optar por investir nas operações cibernéticas (na *espada*) e, principalmente, em operações cibernéticas voltadas à obtenção de divisas, elas auxiliaram (e ainda auxiliam) o Estado a custear a construção das armas. É razoável afirmar que ações ofensivas voltadas à espionagem, como a do furto de documentos da empresa sul-coreana KHNP, podem ter resultado em ganhos para os projetos. Ou seja, o investimento na área cibernética impactou no desenvolvimento das ADM do país.

Corroborando o que foi dito, Perlroth afirma que os ataques da Coreia do Norte são uma forma fácil de contornar as sanções e obter dinheiro, quando comparados aos métodos anteriores (PERLROTH, 2021, p. 335). Chris Inglis, ex-vice-diretor da NSA entre 2006 e 2014, reconhece que o custo de entrada no espaço cibernético é baixo (quando comparado com os demais domínios e com o desenvolvimento de armas de destruição em massa), além de oferecer anonimato e discrição necessários para certas operações. Inglis, inclusive, reconhecia que o programa cibernético norte-coreano é um dos mais bem-sucedidos, nem tanto pela sofisticação (à época), mas porque atinge objetivos com baixo custo. (PERLROTH, 2021, p. 335).

Olhando sob o prisma de avaliação da imagem do país, o uso dessas ações pouco importou. A percepção do país junto aos demais não sofreu tanto impacto, pois em parte era tratado como um "reino eremita", com pouca relevância econômica. E percebo que, possivelmente, nem as sanções impostas pelo Conselho de Segurança da ONU recebiam a atenção devida. O custo, portanto, da imagem do país não parece ter sofrido impacto com o desenvolvimento e aplicação da *espada de múltiplos propósitos*.

Isso subverteu de um modo singular, *sui generis*, a balança de poder. A relevância buscada pelo país não foi obtida diretamente pelo poder cibernético, mas indiretamente, e com um custo muito baixo. Kello (2017, p. 14) afirma que

> [a] arma virtual não está reconfigurando o equilíbrio de poder entre as grandes nações, é apenas uma ferramenta imperfeita de coerção e não alterou a natureza da conquista territorial. No entanto, esta nova capacidade alimenta a disrupção sistêmica porque priva os estados de suposições 'se-então' claras sobre as quais se deve realizar uma moderada disputa por segurança. Embora não altere o equilíbrio de poder, ou

> transforme a natureza da guerra, o domínio cibernético é um terreno reprodutor perfeito para a instabilidade estratégica[177] (KELLO, 2017, p. 14, tradução minha).

Com relação ao afirmado, a Coreia do Norte executou ações imperfeitas de coerção e não foi capaz de conquistar territórios. Mas sua presença no domínio cibernético gerou uma instabilidade, com um certo reequilíbrio de poder. Não entre grandes nações, já que a Coreia do Norte está longe de ser uma. Mas o país se tornou relevante, com o auxílio de suas ações subversivas no espaço cibernético, auxiliando no desenvolvimento das armas estratégicas.

Com relação a trabalhos futuros, este é um estudo de caso único, idiográfico. Não entendo outros casos como sendo semelhantes ao da Coreia do Norte. Assim, não entendo que o estudo consiga ser replicado em outros países. Entretanto, muito há que se continuar observando e, principalmente, ver se o equilíbrio da balança de poder será mantido, considerando que o país possui conexões fortes com suas potências vizinhas Rússia e China, ambos também países detentores de armas estratégicas. Outras questões de possível interesse, relacionadas com o tema da pesquisa, a seguir.

Atividades cibernéticas com objetivo financeiro no domínio cibernético executadas por outros Estados deve ser pesquisada. Caberia uma análise dos atores relevantes, o tipo de ações financeiras executa e, em caso positivo, qual o valor obtido e o possível destino.

Há estudos recentes sobre relacionamentos entre grupos criminosos transnacionais e grupos terroristas em diversas partes do mundo, dentro da teoria do *crime-terror continuum* (MAKARENKO, 2004). Um exemplo desses relacionamentos seria o de grupos terroristas se aliarem a grupos criminosos para obter dinheiro de modo a financiar suas atividades. Ou seja, o crime consiste num meio para se chegar a um fim. Dentro dessa teoria, o estado da Coreia do Norte se mostraria um estado criminoso, situado numa posição que a autora denomina "buraco negro", em que os fins políticos e criminosos estão misturados e não seriam facilmente identificáveis. E é possível que, em certas situações, o país execute alianças com grupos criminosos transnacionais para empreender ações criminosas no espaço cibernético, ou mesmo para ações simples como sacar valores obtidos. Trata-se de algo que ainda não foi observado, mas que deve ser monitorado e que merece investigações mais aprofundadas.

Cabe também observar como a Convenção contra Crimes Cibernéticos da ONU, recentemente aprovada e em vias de ser assinada, será aplicada, mas principalmente nos casos

---

[177] Texto original: "The virtual weapon is not reconfiguring the balance of power among large nations, is only an imperfect tool of coercion, and has not altered the nature of territorial conquest. Nevertheless, the new capability fuels systemic disruption because it deprives states of clear 'if-then' assumptions on which to carry out a restrained contest for security. Although it does not alter the balance of power or transform the nature of war, the cyber domain is a perfect breeding ground for strategic instability."

em que APT ligados ao Estado estão envolvidos. Ela também ainda precisa ser internalizada na legislação de cada país e testada na prática, algo que deve ocorrer nos próximos anos.

Por fim, a atuação precípua na investigação de ataques cibernéticos objetivando ganhos financeiros envolve a segurança pública, sendo incumbência da polícia conduzir investigações, obviamente envolvendo trocas de informações com órgãos militares e de inteligência. Devido à transnacionalidade desse tipo de crime, representações regionais de organismos, como Interpol, Ameripol e Europol, poderiam auxiliar no processo. Caberia verificar a legislação de países envolvidos e, mais importante, qual a capacidade real que os peritos das polícias e seus laboratórios possuem para o combate a esse tipo de crime. Ainda que índices como os da ITU avaliem isso indiretamente, caberiam estudos nesta direção. Não se trata de uma linha de pesquisa direta deste trabalho, mas uma busca por avaliar se é necessária a procura por medidas de construção de capacidades homogêneas entre os órgãos.

É grande o desafio para as nações imposto pela Coreia do Norte quanto aos ataques cibernéticos, inclusive sobre os que objetivam ganho financeiro. Várias atividades destas são crimes cibernéticos, como o furto de dinheiro ou sequestro de computadores (*ransomware*), envolvendo empresas e pessoas físicas sendo alvos de um APT associado a um Estado (DUNN CAVELTY, 2013). A mitigação da ação seria, então, de responsabilidade da polícia e justiça nacionais, as quais não têm poder para retaliar, mas precisam ter a capacidade de conhecimento técnico especializado para analisar, investigar e eventualmente, julgar. No caso de envolver ações contra instituições bancárias, pode-se dizer que se trata de uma ameaça à infraestrutura crítica e, portanto, caberia avaliar a atuação de militares, à luz da legislação adequada. Mas não é razoável dizer que se trataria de um ato de guerra. Esses mesmos ataques com objetivos financeiros não se apresentam como algo contra a segurança nacional, mas sim com o objetivo de lucro (CHOUCRI, 2012). Novamente, se o caso concreto envolver infraestruturas críticas como bancos, poder-se-ia permitir a atuação militar, conforme legislação – outro aspecto que também merece atenção e interesse por parte dos pesquisadores da área.

REFERÊNCIAS

8th LAYER INSIGHTS #46. Money Laundering 101: a chat with Investigative Journalist Geoff White. Entrevistado: Geoff White. Entrevistador: Perry Carpenter. [S. l.]: **The Cyberwire**, 4 jun. 2024. Podcast. Disponível em: https://thecyberwire.com/podcasts/8th-layer-insights/46/notes. Acesso em: 4 jun. 2024.

ABC NEWS. Hillary Clinton's new approach to diplomacy. **ABC News**, 20 fev. 2009. Disponível em: https://abcnews.go.com/Politics/International/story?id=6921007. Acesso em: 5 jun. 2024.

AL JAZEERA. North Korea and Iran sign tech agreement. **Al Jazeera**, 2 set. 2012. Disponível em: https://www.aljazeera.com/news/2012/9/2/north-korea-and-iran-sign-tech-agreement. Acesso em: 24 jun. 2024.

ALMIRANTE, O: Correntes Furiosas. Direção: Han-min Kim, Roteiro: Roteiro Cheol-Hong Jeon, Han-min Kim, Produção: Kim Ham-min. Coreia do Sul: CJ Entertainment, 30 jul. 2014. 127 min.

ALN ganhou dólares e deu Rolex a Kim. **O Estado de S. Paulo**, p. A12, 13 set. 2009.

ARI GROSS, Judah. Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor. **The Times of Israel**, 21 mar. 2018. Disponível em: https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/. Acesso em: 12 jun. 2024.

ARNOLD, Kraesten; PIJPERS, Peter; DUCHEINE, Paul; SCHRIJVER, Peter. Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War. In: RIETJENS, Sebastiaan; PEPERKAMP, Lonneke; ROTHMAN, Maarten (eds.). **Reflections on the Russia-Ukraine War**. Leiden, Países Baixos: University Press, 2024.

ARNOLD, A. **Russia Just Gutted the UN Panel of Experts on North Korea – What Now?** RUSI, 3 abr. 2024. Disponível em: https://rusi.org/explore-our-research/publications/commentary/russia-just-gutted-un-panel-experts-north-korea-what-now. Acesso em: 12 jun. 2024.

ARQUILLA, John; RONFELDT, David. **In Athena's Camp**: Preparing for Conflict in the Information Age. RAND, 2017.

ARQUIVO NACIONAL. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Imprensa Nacional. 2005.

ASTIER, H.; KIRBY, P. Sabotagem? O que se sabe sobre rompimento de cabos submarinos na Alemanha. **BBC News**, 19 nov. 2024. Disponível em: https://www.bbc.com/portuguese/articles/c5ymerpmmryo. Acesso em 28 jan. 2025.

BAKER, P. North Korea shipped arms to Russia for use in Ukraine, U.S. says. **The New York Times**, 13 out. 2023. Disponível em: https://www.nytimes.com/2023/10/13/us/politics/north-korea-weapons-russia-ukraine.html. Acesso em: 24 jun. 2024.

BARBO, Sérgio. Relatos de Resistência (entrevista de Ivan Seixas). **Le Monde Diplomatique**. 20 mar. 2023. Disponível em: https://diplomatique.org.br/relatos-de-resistencia/. Acesso em: 20 dez 2024.

BAR-ZOHAR, Michael; MISHAL, Nissim. **Mossad**: The greatest missions of the Israeli Secret Service. Nova Iorque, NY, EUA: Ecco. 2012.

BEJTLICH, R. What APT is (and what it isn't). **Information Security Magazine**, v. 12, n. 6, pp. 25-30. Jul.-Ago. 2010.

BERMUDEZ, Jr., Joseph. S. **Terrorism**: The North Korean connection. Philadelphia, PA, EUA: Taylor & Francis, 1990.

_____. **A History of Ballistic Missile Development in the DPRK**. Occasional Paper no. 2. Center for Nonproliferation Studies, Monterey Institute of International Studies, 1999.

_____. **A New Emphasis on Operations Against South Korea?** A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau Special Report 4. 38 North. 11 jun. 2010.

_____ SIGINT, EW, and EIW in the Korean People's Army: an overview of Development and Organization. In: MANSOUROV, Alexandre Y. **Bytes and bullets**: information technology revolution and national security on the Korean Peninsula. Cap. 13, pp 234-275. Honolulu, EUA: Asia-Pacific Center for Strategic Studies. 2005.

_____. North Korea's Chemical Warfare Capabilities. **38 North**. 10 out. 2013. Disponível em: https://www.38north.org/2013/10/jbermudez101013/. Acesso em: 12 jun. 2024.

BLUM, Andrew. **Tubes**: Behind the scenes at the Internet. Harlow, Reino Unido: Penguin Books, 2012.

BRANQUINHO, Marcelo Ayres; DE MORAES, Leonardo Cardoso; SEIDL, Jan; DE AZEVEDO Jr., Jarcy; BRANQUINHO, Thiago Braga. **Segurança de automação industrial e SCADA**. 1 ed. Rio de Janeiro: Elsevier, 2014.

BRASIL, Gabinete de Segurança Institucional. **Portaria GSI/PR nº 93**: Aprova o glossário de segurança da informação. Poder Executivo, Brasília, DF. 18 out. 2021.

BRASIL, Ministério da Defesa. **Portaria Normativa nº 9/GAP/MD**: Aprova o Glossário das Forças Armadas – MD35-G-01 (5ª Edição/2015). Poder Executivo, Brasília, DF. 13 jan. 2016.

BRASIL, Presidência da República. **Lei nº 12.965**: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Poder Executivo, Brasília, DF. 23 abr. 2014.

_____. **Lei nº 13.709**: Lei Geral de Proteção de Dados Pessoais (LGPD). Poder Executivo, Brasília, DF. 14 ago. 2018a.

_____. **Decreto nº 9.637**: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Poder Executivo, Brasília, DF. 26 dez. 2018b.

_____. **Decreto nº 10.222**: Aprova a Estratégia Nacional de Segurança Cibernética. Poder Executivo, Brasília, DF. 5 fev. 2020.

_____. **Decreto nº 11.491**: Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Poder Executivo, Brasília, DF. 12 abr. 2023a.

_____. **Decreto nº 11.856**: Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Poder Executivo, Brasília, DF. 11 abr. 2023b.

BREUKER, Remco E. North Korean Slavery and Forced Labor in Present-Day Europe. In: PARGAS, Damian A.; SCHIEL, Juliane (eds.). **The Palgrave Handbook of Global Slavery throughout History**. Cham, Switzerland: Palgrave Macmillan, 2023.

BROWN, Deborah. New UN Cybercrime Treaty Primed for Abuse. **HRW**, 30 dez. 2024. Disponível em: https://www.hrw.org/news/2024/12/30/new-un-cybercrime-treaty-primed-abuse. Acesso em: 20 jan. 2025.

BRUCE, M.; LUSTHAUS, J.; KASHYAP, R.; PHAIR, N.; VARESE F. Mapping the global geography of cybercrime with the World Cybercrime Index. **PLOS ONE**, v. 19, n. 4, 10 abr. 2024.

BUCHANAN, Ben. **The hacker and the state**: Cyber attacks and the new normal of geopolitics. Cambridge, EUA: Harvard University Press, 2020.

BUREAU 39: Kim's Cash Machine (Título original: Büro 39 - Nordkoreas schwarze Kassen). Direção: Sebastian Weis, Lukas Augustin, Carl Gierstorfe. Roteiro: Carl Gierstorfer. Produção: Tristan Chytroschek. Alemanha, 3 fev. 2020. (58 min.) Disponível em: https://youtu.be/s3w96Lr3n7w-vQl. Acesso em: 21 dez. 2024.

BURGIS, Tom. North Korea: The secrets of office 39. **Financial Times**, 24 jun. 2015. Disponível em: https://www.ft.com/content/4164dfe6-09d5-11e5-b6bd-00144feabdc0. Acesso em: 20 dez. 2024.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional**. 1 ed., São Paulo: Editora UNESP. 2012.

C4ADS. **Unmasked**: Vessel Identity Laundering and North Korea's Maritime Sanctions Evasion. 9 set. 2021.

CALTAGIRONE, Sergio; PENDERGAST, Andrew, BETZ, Christopher. **The Diamond Model of Intrusion Analysis**. U.S. Department of Defense Technical Report. Hanover, MD, EUA: Center For Cyber Intelligence Analysis and Threat Research, 2013.

CANABARRO, D. R. **Governança global da Internet**: Tecnologia, Poder e Desenvolvimento. 2014. 432 f. Tese (Doutorado). Programa de Pós-Graduação em Ciência Política, UFRGS, Porto Alegre, 2014.

CANCIAN, Mark F.; PARK, Chris H. **North Korean Troops Deploy to Russia: What's the Military Effect?** CSIS. 25 out. 2024. Disponível em: https://www.csis.org/analysis/north-korean-troops-deploy-russia-whats-military-effect. Acesso em: 4 dez. 2024.

CARLIN, J. **Dawn of the code war**: America's battle against Russia, China, and the rising global cyber threat. Nova Iorque, NY, EUA: PublicAffairs, 2018.

CARLIN, R. L.; LEE, R. M.; 38 NORTH. Understanding Kim Jong Un's Economic Policymaking: Management System Discourse. 12 fev. 2024. Disponível em: https://www.stimson.org/wp-content/uploads/2024/02/Understanding_Kim_Jong_Uns_Economic_Policymaking_.pdf. Acesso em: 14 abr. 2024.

CARPENTER, B.; BAKER, F.; ROBERTS, M. **RFC #2860**: Memorandum of understanding concerning the technical work of the Internet Assigned Numbers Authority, jun. 2000.

CARR, Jeffrey. The myth of the CIA and the trans-Siberian pipeline explosion. **Sofrep**. 9 jun. 2012. Disponível em: https://sofrep.com/news/the-myth-of-the-cia-and-the-trans-siberian-pipeline-explosion/. Acesso em: 27 jan. 2025.

CARVALHO, P. Treta de Coreias: como 600(!) balões com cocô criaram incidente diplomático. **UOL**, 3 jun. 2024. Disponível em: https://noticias.uol.com.br/internacional/ultimas-noticias/2024/06/03/coreia-do-norte-como-balao-com-coco-virou-incidente-diplomatico.htm. Acesso em: 5 jun. 2024.

CERT.BR. **Cartilha Internet Segura**: Códigos Maliciosos. Fascículo. Jul. 2023.

Chaos Computer Club (CCC). **Will Scott**: Computer Science in the DPRK. YouTube, 29 dez. 2014. 33 min 29 s. Disponível em: https://www.youtube.com/watch?v=w703MQZcDhY. Acesso em: 8 dez 2024.

CHA, V.; KIM, E. **The New Russia-North Korea Security Alliance**. CSIS. 20 jun. 2024. Disponível em: https://www.csis.org/analysis/new-russia-north-korea-security-alliance. Acesso em: 26 jun. 2024.

CHAINALYSIS. $2.2 billion stolen from crypto platforms in 2024, but hacked volumes stagnate toward year-end as DPRK slows activity post-July. **Chainalysis blog**. Disponível em: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/. Acesso em: 9 jan. 2025.

CHANLETT-AVERY, Emma; ROSEN, Liana W.; ROLLINS, John W.; THEORARY, Catherine A. **North Korean Cyber Capabilities**: In Brief. CRS Report, 3 ago 2017.

CHEON, SEONG-WHUN. **The Kim Jong-un Regime's "Byungjin" (Parallel Development) Policy of Economy and Nuclear Weapons and the 'April 1st Nuclearization Law'**. Seul, Coréia do Sul: Korea Institute for National Unification (KINU). 2013.

CHOUCRI, Nazli. **Cyberpolitics in International Relations**. The MIT Press, Cambridge, MA, EUA. 2012.

CHOUCRI, Nazli; CLARK, David D. **International Relations in the cyber age**: The co-evolution dilemma. Cambridge, MA, EUA: The MIT Press, 2019.

CILLUFFO, Frank J. **A Global Perspective on Cyber Threats**. Testimony before the U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations. 16 jun. 2015.

CISO Advisor. Três em cada dez brasileiros foram vítimas de crime cibernético. **CISO Advisor**. 30 abr. 2024a. Disponível em: https://www.cisoadvisor.com.br/tres-em-cada-10-brasileiros-foram-vitimas-de-crime-cibernetico/. Acesso em: 27 ago. 2024.

_____. Brasileiros em lavagem de crypto na Argentina. **CISO Advisor**. 26 ago. 2024b. Disponível em: https://www.cisoadvisor.com.br/brasileiros-em-lavagem-de-crypto-na-argentina/. Acesso em: 27 ago. 2024.

CLARK, C. "North Korea is A cyber super power:" former ROK commander. **Breaking Defense**, 23 mai. 2018. Disponível em: https://breakingdefense.com/2018/05/north-korea-is-a-cyber-super-power-former-rok-commander/. Acesso em: 17 jun. 2024.

CLARK, D. **The IETF Mission and Social Contract**. Disponível em: http://www.ietf.org/old/2009/u/ietfchair/ietf-mission.html, 1992. Acesso em: 29 jul. 2019.

CLARKE, R.; KNAKE, R. **Cyber War**: The next threat and what to do about it. Harper Collins, 2010.

_____. **The Fifth Domain**: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin Press. 16 Jul. 2019.

CLAUSEWITZ, Carl von. **On War**. Tradução: J.J. Graham. London, Reino Unido: Repeater, 2019.

CLAUSSEN, Kathleen. Economic cybersecurity law: a short primer. In: Eneken; KERTTUNEN, Mika. **Routledge Handbook of International Cybersecurity**. Cap. 29, pp. 341-353. Abingdon, Reino Unido: Routledge, 2020.

COLEMAN, Gabriella. **Hacker, Hoaxer, Whistleblower, Spy**: The Many Faces of Anonymous. London, New York, NY, EUA: Verso, 2015.

Congressional Research Service (CRS). **North Korea-Russia relations**: current developments. CRS Insight. Washington, DC, EUA. 6 mai. 2024.

Cooperative Cyber Defence Centre of Excellence (CCDCOE). **About us**. Disponível em: https://ccdcoe.org/about-us/. Acesso em: 17 abr. 2024.

CORERA, Gordon. **Cyberspies**: The secret history of surveillance, hacking, and digital espionage. Nova Iorque, NY, EUA: Pegasus, 2015.

CORMODE, Graham; KRISHNAMURTI, Balachander. Key differences between Web 1.0 and Web 2.0. **First Monday**, vol. 13, n. 6, 2 jun. 2008.

CYBERSECURITY TECH ACCORD. **Cybersecurity Tech Accord calls for changes to new UN treaty to prevent damage to global security online**. Press Release, 29 jul. 2024. Disponível em: https://cybertechaccord.org/press-release-cybersecurity-tech-accord-calls-for-changes-to-new-un-treaty-to-prevent-damage-to-global-security-online/. Acesso em: 28 jan. 2024.

DAS, Krishna N.; SPICER, Jonathan. How the New York Fed fumbled over the Bangladesh Bank cyber-heist. **Reunters**. 21 jul. 2016. Disponível em:

https://www.reuters.com/investigates/special-report/cyber-heist-federal/. Acesso em: 28 jan. 2025.

DAVIS, S.B. “Brazil-United States military relations in the early post-World War II era”, **Diálogos**, DHI/UEM, v.6, n. 1, pp. 13-29, 2002.

DE BRITO, Amanda; DE CASTRO, Maria Carolina. O mapeamento documental da segurança e da defesa cibernética da República Popular da China. In: PINTO, Danielle Jacon Ayres; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria (orgs.). **A geopolítica das estratégias em defesa cibernética**: como EUA, China, Rússia e Israel protegem seu ciberespaço. 1 ed., cap. 2, pp. 47-96, Rio de Janeiro: Editora Alpheratz. 2021.

DE CARVALHO, M. S. R. M.; CUKIERMAN, H. L. The dawn of the Internet in Brazil. **IEEE annals of the history of computing**, v. 37, n. 4, p. 54-63, 2015.

DE FIGUEIREDO, Danniel Garcia Barbosa, DE RÊ, Eduardo, DE MENEZES, Thássia Barbosa de. Gigante. Mãos de Aço: As capacidades russas no jogo de poder do ciberespaço. In: PINTO, Danielle Jacon Ayres, PAGLIARI, Graciela de Conti, GRASSI, Jéssica Maria (orgs.). **A geopolítica das estratégias em defesa cibernética**: como EUA, China, Rússia e Israel Protegem seu Ciberespaço. 1 ed., cap. 3, pp. 97-144, Rio de Janeiro: Editora Alpheratz. 2021.

DE ROSA, Cássio Thyone A.; STUMVOLL, Victor Paulo. A Prova: Presunções, vestígios e indícios. In: DE ROSA, Cássio Thyone A.; STUMVOLL, Victor Paulo. **Criminalística**. 8 ed., cap. 4, pp. 89-101, Campinas, SP: Millennium, 2023.

DE SOUZA, Andrea L.F.R. A diplomacia das canhoneiras e o século XXI: uma revisão conceitual. In. **Hoplos**, v. 1, n. 2, pp. 65-81. 2018.

DEIBERT, R. Cyber-security. In: DUNN CAVELTY, M.; BALZACQ, T. (eds.). **Routledge Handbook of Security Studies**. 2 ed., cap. 16, pp. 172-192. Abingdon, Reino Unido: Routledge, 2017.

DEIBERT, R. J., ROHOZINSNKI, R. Risking security: Policies and paradoxes of cyberspace security. **International Political Sociology**, v. 4, n. 1, pp. 15-32, mar. 2010.

DeNARDIS, L. **The global war for Internet governance**. New Haven, CT, EUA: Yale University Press. 2014.

DENNESEN, K., McNAMARA, L., LENZ, D, WEIDEMANN, A., BUENO, A. Insights on cyber threats targeting users and enterprises in Brazil. **Google Cloud Blog**, 12 jun. 2024. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil. Acesso em: 14 jun. 2024.

DER DERIAN, J. **Virtuous war**: Mapping the military-industrial-media-entertainment network. 2 ed., Nova Iorque, NY, EUA: Routledge, 2009.

Defense Intelligence Agency (DIA). **North Korea military power**: a growing regional and global threat. Washington, DC, EUA: U.S. Government Publishing Office, 2021.

DI NICOLA, G. Investigación del FBI. La ruta de una ciberestafa de norcoreanos que terminó en el departamento de un ruso en Palermo. **La Nación**, 22 ago. 2024. Disponível em:

https://www.lanacion.com.ar/seguridad/investigacion-del-fbi-la-ruta-de-una-ciberestafa-de-norcoreanos-que-termino-en-el-departamento-de-un-nid21082024/. Acesso em: 9 jan. 2025.

DIPLOFOUNDATION. **Digital diplomacy in 2024**. DiploFoundation, 2023. Disponível em: https://www.diplomacy.edu/topics/digital-diplomacy/. Acesso em: 6 mar. 2024.

Director of National Intelligence (DNI). **Background Briefing with Senior U.S. Officials on Syria's Covert Nuclear Reactor and North Korea's Involvement**. 24 abr. 2008. Disponível em: https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20080424_interview.pdf. Acesso em: 12 jun. 2024.

_____. **Annual Threat Assessment of the U.S. Intelligence Community**. 5 fev. 2024. Disponível em: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf. Acesso em: 12 dez. 2024.

DOMINGO, Francis C. Cyberspace. In: FONG, Brian C.H.; CHONG, Ja Ian. **Routledge Handbook of Great Power Competition**. Cap. 5, pp. 265-276. Abingdon, Reino Unido: Routledge, 2025.

DONOVAN, Joan. Refuse and Resist. In: COLEMAN, Gabriella; KELTY, Christopher M. (eds.). **Limn**: Hacks, Leaks, and Breaches, issue no. 8 pp 39-43, fev, 2017.

DUNN CAVELTY, M. **Cyber-Security and threat politics**: US efforts to secure the information age. Routledge, 2008.

_____. The militarisation of cyberspace: why less may be better. In: CZOSSECK, C.; OTTIS, R.; ZIOLKOWSKI K. (eds.). **4th International Conference on Cyber Conflict**. Tallinn, Estônia: NATO CCDCOE Publications, 2012.

_____. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. **International Studies Review**, v. 15, pp. 105–122, 2013.

_____. Cybersecurity between hypersecuritization and technological routine. In: TIKK, Eneken; KERTTUNEN, Mika. **Routledge Handbook of International Cybersecurity**. Cap. 1, pp. 11-21. Abingdon, Reino Unido: Routledge, 2020.

Economist Intelligence Unit, The (EIU). **Democracy Index 2023**: Age of Conflict. 2024.

EGLOFF, Florian J. **Semi-state Actors in Cybersecurity**. Nova Iorque, NY, EUA: Oxford University Press, 2022.

Electronic Frontier Foundation (EFF). **As UN Cybercrime Treaty Negotiations Enter Final Phase, Time is Running Short to Bolster Human Rights Protections**. Media Briefing, 18 ago. 2023. Disponível em: https://www.eff.org/press/releases/media-briefing-un-cybercrime-treaty-negotiations-enter-final-phase-time-running-short. Acesso em: 02 fev. 2025.

European Union Agency for Cybersecurity (ENISA). **ENISA Threat Landscape**: July 2023 to June 2024. Set. 2024.

ESKEW, Carter. The hermit-in-chief. **The Washington Post**, 18 jan. 2019. Disponível em: https://www.washingtonpost.com/news/opinions/wp/2019/01/18/the-hermit-in-chief/. Acesso em: 5 jun. 2024.

Estados Unidos da América (EUA), Casa Branca. **Executive Order 13010**: Critical Infrastructure Protection. 15 jul. 1996.

_____. **United States of America v. JIN HYOK PARK**. CRIMINAL COMPLAINT. 8 jun. 2018b.

_____. **National Cyber Strategy of The United States of America**. Set. 2018b. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 15 mar. 2019.

_____. **National Cyber Strategy**. 1 mar. 2023a. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Acesso em: 11 mai. 2024.

_____, Department of Army. **North Korean Tactics**. Washington, DC, EUA: Army Techniques Publication, 24 jul. 2020.

_____, Department of Defense. **DoD Dictionary of Military and Associated Terms**. Nov. 2021.

_____, Department of Treasury. **Treasury disrupts north Korean digital assets money laundering network**. 17 dez 2024a. Disponível em: https://home.treasury.gov/news/press-releases/jy2752. Acesso em: 9 jan. 2025.

_____, Office of the Director of National Intelligence. **Annual Threat Assessment of the U.S. Intelligence Community**. 5 fev. 2024b. Disponível em: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf. Acesso em: 17 jun. 2024.

_____, Office of Public Affairs. **Justice department announces court-authorized action to disrupt illicit revenue generation efforts of Democratic People's Republic of Korea information technology workers**. U.S. Department of Justice. 18 out. 2023b. Disponível em: https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation. Acesso em: 24 jun. 2024.

_____, Office of the Secretary of Defense. **Military and Security Developments Involving the Democratic People's Republic of Korea 2017**: Report to Congress. 2017. Disponível em: https://irp.fas.org/world/dprk/dod-2017.pdf. Acesso em: 17 jun. 2024.

_____, United States Cyber Command. **Command history**. S.d.a. Disponível em: https://www.cybercom.mil/About/History/. Acesso em: 4 dez. 2024.

_____, United States Cyber Command. **Mission and vision**. S.d.b. Disponível em: https://www.cybercom.mil/About/Mission-and-Vision/. Acesso em: 4 dez. 2024.

EVANS, Dave. **The Internet of Things**: How the Next Evolution of the Internet Is Changing Everything. White Paper. Cisco Internet Business Solutions Group (IBSG), abr. 2011. Disponível em:

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Acesso em: 30 nov. 2024.

FALCONBRIDGE, Guy. Exclusive - North Korean leaders used Brazilian passports to apply for Western visas: sources. **Reuters**. 27 fev. 2018. Disponível em: https://www.reuters.com/article/world/exclusive-north-korean-leaders-used-brazilian-passports-to-apply-for-western-v-idUSKCN1GB2AZ/. Acesso em: 2 jan. 2025.

Federal Bureau of Investigation (FBI). **FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft**. 23 jan. 2023. Disponível em: https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft. Acesso em: 28 dez. 2024.

_____. **Internet Crime Report 2023**. 4 abr. 2024a. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. Acesso em: 9 jun. 2024.

_____. **Alert Number: I-051624-PSA**: Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue. 16 mai. 2024b. Disponível em: https://www.ic3.gov/PSA/2024/PSA240516. Acesso em: 20 jan. 2024.

_____. **Alert Number: I-090324-PSA**: North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks. 3 set. 2024c. Disponível em: https://www.ic3.gov/PSA/2024/PSA240903. Acesso em: 20 jan. 2024.

_____. **Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue**. U.S. Department of Justice. 16 mai. 2024b. Disponível em https://www.ic3.gov/Media/Y2023/PSA231018. Acesso em: 19 jun. 2024.

FERAZZA, Francesco Maria. **Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model**: a comparison of cyber intrusion analysis models. Dissertação (Mestrado), Information Security Group, University of London, Surrey, Reino Unido, 11 abr. 2022.

Financial Stability Board. **Cyber Lexicon**. 12 nov. 2018.

Fundo Monetário Internacional (FMI). **World Economic Outlook**. Abr. 2024a.

_____. **Global Financial Stability Report**: The Last Mile: Financial Vulnerabilities and Risks. Abr. 2024b.

FLECK, Anna. Cybercrime expected to skyrocket in coming years. **Statista**, 22 fev. 2024. Disponível em: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/. Acesso em: 18 jun. 2024.

FOLLATH, E.; STARK, H. The story of “operation orchard”: How Israel destroyed Syria’s Al kibar nuclear reactor. **Der Spiegel**, 2 nov., 2009. Disponível em: https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html. Acesso em: 12 jun. 2024.

FONSECA, João José de Saraiva. **Apostila de metodologia da pesquisa científica**. Fortaleza: UECE, 2002.

FORNAZARI JÚNIOR, Milton. **Cooperação jurídica internacional**: atribuições legais no auxílio direto. Revista Brasileira de Ciências Policiais, v. 6, n. 2, pp. 217-234. Brasília, jul. 2015.

FRANCESCHI-BICCHIERAI, L. North Korea has just 28 websites. **Motherboard**, 20 set. 2016. Disponível em: https://www.vice.com/en/article/ezpm7z/north-korea-has-just-28-websites. Acesso em: 9 mar. 2024.

_____. The North Korean Facebook clone has already been hacked. **Motherboard**, 27 mai. 2016a. Disponível em: https://www.vice.com/en/article/78kkq9/the-north-korean-facebook-clone-has-already-been-hacked. Acesso em: 9 mar. 2024.

FUTTER, A. **Hacking the bomb**: Cyber threats and nuclear weapons. Washington, DC, EUA: Georgetown University Press, 2018.

GARTZKE, Erik; LINDSAY, John R. The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence. In: LIN, Herbert; ZEGART, Amy. **Bytes, Bombs, and Spies**: The Strategic Dimensions of Offensive Cyber Operations. Washington, DC, EUA: Brookins Institution Press, 2018.

GARVEY, Myles D. A Philosophical Examination on the Definition of Cyberspace. In: CARNOVALE, Steven; YENIYURT, Sengun. **Cyber Security and Supply Chain Management**: Risks, Challenges, and Solutions, vol. 1, cap. 1, pp. 1-11. Singapura: World Scientific Publishing Company, 2021.

GASPAR, João Alberto Muniz. **Ransomware**. Orientação de Segurança da Informaçãoo e Cibernética (OSIC) 14/2023. Brasília, DF: Gabinete de Segurança Institucional/Presidência da República, 17 out. 2023.

GATES, Bill. Bill Gates: Trustworthy computing. **Wired**, 17 jan. 2002. Disponível em: https://www.wired.com/2002/01/bill-gates-trustworthy-computing/. Acesso em: 2 fev. 2025.

GERRING, John. **Case Study Research**: Principles and Practices. Cambridge, Reino Unido: Cambridge University Press, 2007.

GIBSON, William. **Neuromancer**. Tradução Fábio Fernandes. 5 ed. São Paulo: Editora Aleph, 2016.

GILES, Keir. Russia and its neighbors: old attitudes, new capabilities. In: GEERS, Kenneth. (ed.) **Cyber war in perspective**: Russian aggression against Ukraine. Tallinn, Estônia: NATO CCDCOE Publications. 2015.

GILES, Keir; HAGESTAD II, William. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In: PODINS, K; STINISSEN, J.; MAYBAUM, M. (eds.). **5th International Conference on Cyber Conflict**. Tallinn, Estônia: NATO CCDCOE Publications, 2013.

GODOY, Marcelo. Coreia treinou guerrilha brasileira. **O Estado de S. Paulo**, p. A12, 13 set. 2009.

_____. **A casa da vovó**: Uma biografia do DOI-Codi (1969-1991), o centro de seqüestro, tortura e morte da ditadura militar. São Paulo: Editora Alameda, 2014.

GOLDSMITH, Jack; WU, Tim. **Who controls the Internet?** Illusions of a borderless world. New York: Oxford University Press, 2006.

GONZALES, A. A. **Quem governa a Governança da Internet?** Uma análise do papel da Internet sobre os rumos do sistema-mundo. 2016. 75f. Dissertação (Mestrado) Programa de Pós-Graduação em Ciência Política, UFRGS, Porto Alegre, 2016.

GOODMAN, M. **Future crimes**: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. 1 ed., HSM Editora, 2 mai. 2018.

GREENBERG, A. North Korea hacked him. So he took down its Internet. **Wired**, 2 fev. 2022. Disponível em: https://www.wired.com/story/north-korea-hacker-internet-outage. Acesso em: 7 mar. 2024.

_____. A Vigilante Hacker Took Down North Korea's Internet. Now He's Taking Off His Mask. **Wired**, 4 abr. 2024. Disponível em: https://www.wired.com/story/p4x-north-korea-internet-hacker-identity-reveal/. Acesso em: 4 abr. 2024.

_____. **Sandworm**: A new era of cyberwar and the hunt for Kremlin's most dangerous hackers. 1 ed., Nova Iorque, NY, EUA: Doubleday, 2019.

GREENWALD, Glenn. **Sem lugar para se esconder**. Tradução: Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

GREIG, Jonathan. Controversial UN cybercrime treaty clears final hurdle before full vote as US defends support. **The Record**, 12 nov. 2024. Disponível em: https://therecord.media/un-cybercrime-treaty-clears-vote. Acesso em: 28 jan. 2024.

GREITENS, Sheena Chestnut. **Illicit**: North Korea's Evolving Operations to Earn Hard Currency. Washington, DC, EUA: Committee for Human Rights in North Korea, 2014.

GRIFFIS, W. E. Corea, the Hermit Nation. **Journal of the American Geographical Society of New York**, v. 13, pp. 125-132, 1881.

GRIZENDI, Eduardo; STANTON, Michael. A rede da RNP e novas parcerias. In: KNIGHT, Peter; FEFFERMAN, Flávio; FODITSCH, Nathália (orgs.). **Banda Larga no Brasil**: passado, presente e futuro. Cap. 9, pp. 209-247. São Paulo: Figurati, 2016.

GROMOV, G. **The Roads and Crossroads of the Internet History**. 1995. Disponível em: http://history-of-internet.com/history_of_internet.pdf. Acesso em: 14 jun. 2024.

GUISNEL, Jean. **CyberWars:** espionage on the Internet. Tradução: Gui Massai. Basic Books, EUA. 1999.

HAGAN, Rachel. Pentagon responds to claims North Korean troops in Russia 'gorging on pornography'. **Independent**, 8 nov. 2024. Disponível em: https://www.independent.co.uk/news/world/europe/north-korean-internet-porn-ukraine-russia-war-b2643549.html. Acesso em: 4 dez. 2024.

HARDING, Luke. Suicides, new tactics and propaganda iPads: details from captured North Koreans expose new foe in Ukraine. **The Guardian**, 18 jan. 2025. Disponível em:

https://www.theguardian.com/world/2025/jan/18/suicides-new-tactics-and-propaganda-ipads-details-from-captured-north-koreans-expose-new-foe-in-ukraine. Acesso em: 19 jan. 2025.

HAROLD, Scott; BEAUCHAMP-MUSTAFAGA, Nathan; JUN, Jenny; MYERS, Diana. **Will Artificial Intelligence Hone North Korea's Cyber "All-Purpose Sword"?** Special Report 7. Washington, DC, EUA: Korea Economic Institute. 2 mar. 2022.

HARRIS, Shane. **@War**: The rise of the Military-Internet Complex. Mariner Books, 2015.

HASSAN, Tirana. Upcoming Cybercrime Treaty Will Be Nothing But Trouble. **Foreign Policy in Focus**. Disponível em: https://fpif.org/upcoming-cybercrime-treaty-will-be-nothing-but-trouble/. Acesso em: 28 jan. 2025.

HEGEL, Tom. Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company. **SentinelOne**, 7 ago. 2023. Disponível em: https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/. Acesso em: 17 jun. 2024.

Hewlett Packard (HP) Security Research. **Profiling an enigma**: The mystery of North Korea's cyber threat landscape. HP Security Briefing, Episode 16. Ago. 2014.

HINOJOSA, Pablo; AIKEN, Klée; HUREL, Louise Marie. Putting the Technical Community Back into Cyber (Policy). In: TIKK, Eneken; KERTTUNEN, Mika. **Routledge Handbook of International Cybersecurity**. Cap. 28, pp. 326-340. Abingdon, Reino Unido: Routledge, 2020.

HÖNÖ, Ölli. **From Moonlight Maze to Solarwinds**: How Russian APT Groups Operate? 131 pp. Tese (Mestrado), Jyväskylä, Finlândia: University of Jyväskylä, 2023.

Human Rights Watch (HRW). **UN: Draft Cybercrime Treaty Threatens Rights**. 23 jan. 2024. Disponível em: https://www.hrw.org/news/2024/01/23/un-draft-cybercrime-treaty-threatens-rights. Acesso em: 28 fev. 2025.

HSU, Kimberly; MURRAY, Craig. **China and International Law in Cyberspace**. U.S.-China Economic and Security Review Commission Staff Report, 6 mai. 2014.

HUREL, Louise Marie. **Cibersegurança no Brasil**: uma análise da estratégia nacional. Artigo Estratégico 54. Instituto Igarapé, abr. 2021.

International Campaign to Abolish Nuclear Weapons (ICAN). **Surge**: 2023 Global nuclear weapons spending. Report. Genebra, Suíça: ICAN, jun.2024.

INTERNATIONAL CRISIS GROUP. North Korea's chemical and biological weapons program. **Asia Report**, n. 167. 18 jun. 2009.

International Telecommunications Union (ITU). **Global Cybersecurity Index (GCI) 2020**. 4 ed., ITU. 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 9 jun. 2024.

_____. **Measuring digital development Facts and Figures 2023**. ITU. 2023. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2023-1-pdf-e.pdf. Acesso em: 9 jun. 2024.

_____. **Global Cybersecurity Index (GCI) 2024**. 5 ed., ITU. 2024. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf. Acesso em: 8 jun. 2024.

Internet World Stats (IWS) **Asia internet stats by country and population statistics**. 31 jan. 2024. Disponível em: https://www.internetworldstats.com/asia.htm#kp. Acesso em: 20 abr. 2024.

INTERPOL. **Ag-2006-RES-04**: Statement to Reaffirm the Independence and political Neutrality of Interpol. Rio de Janeiro. Set. 2006.

_____. **Innovation centre catalogue of services**. Singapura, set. 2022.

_____. **The Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session**. Vienna. 2023.

IZYCKI, E. A. **Cyber offensive capabilities**: A glimpse on a multipolar dimension. 2021. 359 pp. Dissertação (Mestrado), Programa de Pós-Graduação em Relações Internacionais, UnB, 2021.

JACOBSEN, Jeppe T. Europe Is Developing Offensive Cyber Capabilities. The United States Should Pay Attention. **CFR Blog**, 26 abr. 2017. Disponível em: https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention. Acesso em: 5 fev. 2025.

JAKES, L. What weapons is North Korea accused of supplying to Russia? **The New York Times**, 17 jun. 2024. Disponível em: https://www.nytimes.com/2024/06/17/world/europe/russia-north-korea-weapons-ukraine.html. Acesso em: 26 jun. 2024.

JEONG, Andrew. North Korean Hackers Are Said to Have Targeted Companies Working on Covid-19 Vaccines. **Wall Street Journal**. 2 dez. 2020. Disponível em: https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026. Acesso em: 27 nov. 2024.

JERVIS, Robert. **The Logic of Images in International Relations**. Princeton, NJ, EUA: Columbia University Press, 1970.

JIANG, H. Cybersecurity Domain Map ver 3.0. **Linkedin**, 11 mar. 2021. Disponível em: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/. Acesso em: 2 fev. 2024.

JI-YOUNG, K.; JONG IN, L.; KYOUNG GON, K. The all-purpose sword: North Korea's cyber operations and strategies. In: **Proceedings 11th International Conference on Cyber Conflict: Silent Battle**. Tallinn, Estônia: NATO CCDCOE Publications, mai. 2019.

JOGOS de Guerra. Direção: John Badham, Produção: United Artists Pictures Inc. (Transamerica Corp.). Estados Unidos: Metro-Goldwyn-Mayer, 1983. 1 DVD. (114 min.)

JONES, Seth G. **Three dangerous men**: Russia, China, Iran and the rise of irregular warfare. Nova Iorque, NY, EUA: W.W. Norton & Company, 2023.

JUN, Jenny; LAFOY, Susan; SOHN, Ethan. **North Korea's Cyber Operations**: Strategy and Responses. CSIS, dez. 2015.

KAN, P. R.; BECHTOL, B. E.; COLLINS, R. M. **Criminal sovereignty**: Understanding North Korea's illicit international activities. Carlisle, PA, EUA: Strategic Studies Institute, U.S. Army War College. mar. 2010.

KANG, Taejun. N Korea attempts to hack Russian foreign ministry: report. **Radio Free Asia**, 22 fev. 2024. Disponível em: https://www.rfa.org/english/news/korea/nk-russia-hack-02222024003639.html. Acesso em: 17 jun. 2024.

KAPLAN, Fred. **Dark Territory**: The secret history of cyber war. Nova Iorque, NY, EUA: Simon & Schuster, 2016.

KASPERSKY. O que é doxing: é ilegal? Como evitar? **Kaspersky**. 7 nov. 2020. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-doxing. Acesso em: 28 jan. 2025.

KASZETA, Dan. **Toxic**: a history of nerve agents, from Nazi Germany to Putin's Russia. Oxford, Reino Unido: Oxford University Press, 2021.

KECK, Zachary. S. Korea Seeks Cyber Weapons to Target North Korea's Nukes. **The Diplomat**. 21 fev. 2014. Disponível em: https://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/. Acesso em: 27 nov. 2024.

KELLO, Lucas. **The Virtual Weapon and International Order**. New Haven, CT, EUA: Yale University Press, 2017.

KESSLER, Gary D.; SHEPARD, Steven D. **Maritime Cybersecurity**: A Guide for Leaders and Managers. 2 ed. (versão e-book 2.3, jan. 2025), 2020.

KILCULLEN, D. **The dragons and the snakes**: How the rest learned to fight the west. Nova Iorque, NY, EUA: Oxford University Press, 2020.

KIM, Chong Woo; POLITO, Carolina. **The Evolution of North Korean Cyber Threats**. Issue Brief. The Asian Institute for Policy Studies, 19 fev. 2019.

Kim Jong-il's escape plan. **Pyongyang Papers**. 28 set. 2018. Disponível em: https://pyongyangpapers.com/investigations/kim-jong-ils-escape-plan/. Acesso em: 4 jan. 2025.

KIM, Joon Ho. Cibernética, Ciborgues e Ciberespaço: Notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes Antropológicos**, Porto Alegre, ano 10, n. 21, pp. 199-219, jan. 2004.

KIM, Hyun-kyung; PHILLIP, Elizabeth; CHUNG, Hattie. **North Korea's Biological Weapons Program**: The known and unknown. Report. Cambridge, MA, EUA: Belfer Center for Science and International Affairs. Out. 2017.

KIM, Hyung-jin.; KIM, Tong-hyung. North Korea spy satellite launch fails as rocket falls into the sea. **The Diplomat**, 1 jun. 2023. Disponível em: https://thediplomat.com/2023/06/north-korea-spy-satellite-launch-fails-as-rocket-falls-into-the-sea/. Acesso em: 27 nov. 2024.

KIM, Suki. **Without You, There Is No Us**: My time with the sons of North Korea's elite. Nova Iorque, NY, EUA: Crown. 2014.

KIM, Sung-han. No denuclearization, no peace. **Korea JoongAng Daily**, 16 ago. 2020. Disponível em: https://koreajoongangdaily.joins.com/2020/08/16/opinion/columns/195053-Korean-War/20200816193600298.html. Acesso em: 15 jun. 2024.

KIM, Sung-han; LEE, Alex Soonhon. Security and Defence Policy. In: HAN, Jeonghun; PACHECO-PARDO, Ramon; CHO, Younghjo. (eds.) **The Oxford Handbook of Korean Politics**. Oxford, Reino Unido: Oxford University Press, 2023.

KIM, Tong-hyung. South Korean defense chief says North Korea has supplied 7,000 containers of munitions to Russia. **The Associated Press**, 18 mar. 2024. Disponível em: https://apnews.com/article/north-korea-russia-arms-transfers-ukraine-a37bc290ed3ee59cfbbafdc2a994dc58. Acesso em: 17 jun. 2024.

KIMBAL, Daryl G. North Korea and the incident in the Syrian desert. **Arms Control Association**, mai. 2008. Disponível em: https://www.armscontrol.org/act/2008-05/issue-briefs/north-korea-and-incident-syrian-desert. Acesso em: 24 jun. 2024.

KLEINROCK, L. An early history of the Internet. **IEEE Communications Magazine**, v. 48, n. 8, pp. 26-36, 2010.

KONG, Ji Young; LIM, Jong In; KIM, Kyoung Gon. The All-Purpose Sword: North Korea's Cyber Operations and Strategies. **11th International Conference on Cyber Conflict**: Silent Battle. Tallinn, Estônia: NATO CCDCOE Publications, 2019.

KOVACS, Eduard. U.S., Canada, Australia Attribute NotPetya Attack to Russia. **Security Week**, 16 fev. 2018. Disponível em: https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia/. Acesso em: 5 jun. 2024.

KREBS, Brian. Indian bank hit in $13.5M cyberheist after FBI ATM cashout warning. **Krebs on Security**, 17 ago. 2018. Disponível em: https://krebsonsecurity.com/2018/08/indian-bank-hit-in-13-5m-cyberheist-after-fbi-atm-cashout-warning/. Acesso em: 28 jan. 2025.

KRISTENSEN, H.; KORDA, M.; JOHNS, E.; KNIGHT, M.; KOHN, K. **Status of World Nuclear Forces**. Federation of American Scientists, 26 mar. 2024. Disponível em: https://fas.org/initiative/status-world-nuclear-forces/. Acesso em: 12 jun. 2024.

KROPOTOV, Vladimir; LIN, Philippe, YAROCHKIN; Fyodor; HACQUEBORD, Feike. A Closer Look at North Korea's Internet. **Trend Micro**, 17 out. 2017. Disponível em: https://www.trendmicro.com/en_us/research/17/j/a-closer-look-at-north-koreas-internet.html. Acesso em: 8 mar. 2024.

KU, Yangmo. An effective shield? Analyzing South Korea's cybersecurity strategy. In: RUMANIUK, Scott N., MANJIKIAN, Mary (eds.). **Routledge companion to global cyber-security strategy**. Cap. 22, pp. 267-275. Abingdon, Reino Unido: Routledge, 2021.

KUEHL, D. T. From Cyberspace to Cyberpower: defining the problem. In: KRAMER, F.; STARR, S.; WENTZ, L. (eds.). **Cyberpower and national security**. Washington, DC, EUA: National Defense University. 2009.

KURBALIJA, Jovan. **An introduction to Internet governance**. 7 ed., Genebra, Suíça: DiploFoundation, 2016.

KUZIN, Eugen; KRUPYSHEV, Max. The CoinsPaid hack explained: We know exactly how attackers stole and laundered $37M USD. **Coinspaid**, 7 ago. 2023. Disponível em: https://coinspaid.com/company-updates/the-CoinsPaid-hack-explained/. Acesso em: 3 fev. 2025.

LANG, Jack. The tiny Brazilian club that fooled North Korea – 'They would have been angry if we had won'. **The New York Times**, 27 fev. 2024. Disponível em: https://www.nytimes.com/athletic/5279281/2024/02/27/brazil-north-korea-atletico-sorocaba/. Acesso em: 21 dez. 2024.

LANGEWIESCHE, William. **O bazar atômico**: A escala do pobrerio nuclear. Tradução José Viegas. São Paulo: Companhia das Letras. 2007.

LEARY, Timothy. The Cyber-Punk: the individual as reality pilot. **Mississippi Review**, vol. 16, n. 2/3, p. 252-265. University of Southern Mississippi, 1988.

LEE, H. Y. South Korea in 2003: *A question of leadership?* **Asian survey**, v. 44, n. 1, pp. 130-138, 2004.

LEE, Seungmin (Helen). Revisiting the 2014 Korea Hydro and Nuclear Power Hack: Lessons Learned for South Korean Cybersecurity. **38 North**. Disponível em: https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity/. Acesso em: 27 jan. 2025.

LESSIG, L. **Code v. 2.0**. Nova Iorque, NY, EUA: Basic Books. 2006.

LEVKOWITZ, Alon. **North Korea and the Middle East**. Mideast Security and Policy Studies no. 127. Ramat Gan, Israel: Bar-Ilan University, The Begin-Sadat Center for Strategic Studies, Bar-Ilan University, jan. 2017.

LÉVY, Pierre. **Cibercultura**. Tradução: Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LI, Alex. Digital piracy returns to sea: Protecting autonomous ships from online attacks. **War on the Rocks**. 6 out. 2023. Disponível em: https://warontherocks.com/2023/10/digital-piracy-returns-to-sea-protecting-autonomous-ships-from-online-attacks/. Acesso em: 7 out. 2024.

LIN, Herbert. Attribution of Malicious Cyber Incidents: From Soup to Nuts. In: **Journal of International Affairs**, vol. 70, n. 1, pp 75-137, 2 set. 2016.

MADHANI, A.; LEDERER, E. M. White House: Russia's Wagner received arms from North Korea. **AP News**, 23 dez. 2022. Disponível em: https://apnews.com/article/russia-ukraine-business-north-korea-e6a068d91bc9828ecadfb67c929a4162. Acesso em: 24 jun. 2024.

MAKARENKO, Tamara. The crime terror continuum: tracing the interplay between transnational organized crime and terrorism. In: **Global Crime** v. 6, n. 1, pp. 129-145. Londres, Reino Unido: Routledge, fev. 2004.

MALLONEY, S. What is an Advanced Persistent Threat (APT)? **Cybereason blog**, [s.d.]. Disponível em: https://www.cybereason.com/blog/advanced-persistent-threat-apt. Acesso em: 9 jan. 2024.

MANDIANT. **APT1**: Exposing One of China's Cyber Espionage Units. 18 fev. 2013. Disponível em: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf. Acesso em: 9 abr. 2024.

MANEKI, Sharon A. **Learning from the Enemy**: The GUNMAN Project. 2 ed. Fort George G. Meade, MD, EUA: Center for Cryptologic History, 2018.

MANESS, Ryan C.; VALERIANO, Brandon. **Russia's Coercive Diplomacy**: Energy, Cyber, and Maritime Policy as New Sources of Power. Palgrave Macmillan, 2015.

MARCONDES, Danilo. Distant Friends? Twenty Years of Brazil–DPRK Diplomatic Relations (2001–2021). **North Korean Review**, v. 18, n. 2, pp. 5-20, 2022.

MARTIN, Bradley K. **Under the loving care of the fatherly leader**: North Korea and the Kim dynasty. 1 ed., Nova Iorque, NY, EUA: Thomas Dunne Books, set. 2004.

MCWILLIAMS, Brian. North Korea's school for hackers. **Wired**, 2 jun. 2003. Disponível em: https://www.wired.com/2003/06/north-koreas-school-for-hackers/. Acesso em: 7 mar. 2024.

VISENTINI, Paulo G. Fagundes; PEREIRA, Analúcia Danilevicz; MELCHIONNA, Helena Hoppen. **A Revolução Coreana**: O desconhecido socialismo Zuche. São Paulo: Editora Unesp, 2015.

MELMAN, Yossi; RAVIV, Dan. Three minutes over Syria: How Israel destroyed Assad's nuclear reactor. **The Times of Israel**, 21 mar. 2018. Disponível em: https://www.timesofisrael.com/three-minutes-over-syria-how-israel-destroyed-assads-nuclear-reactor/. Acesso em: 12 jun. 2024.

MEMORIAL DA RESISTÊNCIA. **Darci Toshiko Miyaki**. Disponível em: https://memorialdaresistenciasp.org.br/pessoas/darci-toshiko-miyaki/. Acesso em: 20 dez. 2024.

MENN, J. Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources. **Reuters**. 29 mai. 2015. Disponível em: https://www.reuters.com/article/idUSKBN0OE2DM/. Acesso em: 21 abr. 2024.

MICROSOFT. **Microsoft Digital Defense Report 2022**. Microsoft Threat Intelligence. 4 nov. 2022.

_____. **Microsoft Digital Defense Report 2023**. Microsoft Threat Intelligence, out. 2023.

_____. **Microsoft Digital Defense Report 2024**. Microsoft Threat Intelligence, out. 2024.

MILLER, Greg; DIXON, Robin; STANLEY-BECKER, Isaac. Accidents, not Russian sabotage, behind undersea cable damage, officials say. **The Washington Post**, 19 jan. 2025. Disponível em: https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/. Acesso em: 27 jan. 2025.

MILLER, Nicholas S.; NARANG, Vipin. How North Korea Shocked the Nuclear Experts. **Polito Magazine**. 26 ago. 2017. Disponível em: https://www.politico.com/magazine/story/2017/08/26/north-korea-nuclear-tests-shock-experts-215533/. Acesso em: 24 jan. 2025.

MISSILE DEFENSE PROJECT. SS-1 "Scud". *Missile Threat*. CSIS, 23 abr. 2024. Disponível em: https://missilethreat.csis.org/missile/scud/. Acesso em: 14 jan. 2025.

MIYAKI, Darci Toshiko. **Entrevista com Darci Toshiko Miyaki**. São Paulo: Memorial da Resistência de São Paulo, entrevista concedida a Karina Alves e Ana Paula Brito em 24 de abril de 2014, 3 h 6 min.

MORGAN, Steve. Top 10 cybersecurity predictions and statistics for 2024. **Cybercrime Magazine**, 5 fev. 2024. Disponível em: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/. Acesso em: 18 jun. 2024.

MORGENTHAU, Hans J. **A política entre as nações**: a luta pela guerra e pela paz Brasília, DF: Editora UnB. 2003.

MORTON, B.; BEALE, J.; GRAMMATICAS, D. UK warns Putin after Russian spy ship seen near British waters. **BBC**, 22 jan. 2025. Disponível em: https://www.bbc.com/news/articles/cqjv7qgpw28o. Acesso em: 28 jan. 2025.

MOZUR, Paul; SANG-HUN, Choe. North Korea's rising ambition seen in bid to breach global banks. **The New York Times**, 25 mar. 2017. Disponível em: https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html. Acesso em 27 jan. 2025.

MUELLER, M. **Ruling the Root**: Internet governance and the taming of cyberspace. Cambridge, MA: MIT Press. 2002.

MUNDIE, Craig; DE VRIES, Pierre; HAYNES, Peter; CORWINE, Matt. **Trustworthy Computing**. Microsoft White Paper, out. 2002. Disponível em: http://download.microsoft.com/documents/australia/about/trustworthy_comp.doc. Acesso em: 2 fev. 2025.

MUNERATTO, G. O Homem de 6 Milhões de Dólares: Como série famosa inspirou a ciência? Tangerina. 7 mar. 2023. Disponível em: https://tangerina.uol.com.br/filmes-series/o-homem-de-6-milhoes-de-dolares-50-anos/. Acesso em: 22 set. 2024.

NEGROPONTE, Nicholas. **A Vida Digital**. Companhia das Letras. 1995.

NEWMAN, L. H. North Korea targets—and dupes—a slew of cybersecurity pros. **Wired**, 26 jan. 2021. Disponível em: https://www.wired.com/story/north-korea-hackers-target-cybersecurity-researchers/. Acesso em: 7 mar. 2024.

NEWTON, Matthew; PARK, Donghui. Russia Is Now Providing North Korea With Internet: What That Could Mean For Cyber Warfare. **Forbes**, 11 dez. 2017. Disponível em: https://www.forbes.com/sites/outofasia/2017/12/01/russia-is-now-providing-north-korea-with-internet-what-that-could-mean-for-cyber-warfare/. Acesso em: 30 jan. 2017.

NOLAND, Marcus. Telecommunications in North Korea: Has Orascom made the connection? **North Korean Review**, v. 5, n. 1, pp. 62–74, 2009.

North Korea's Secret Slaves: Dollar Heroes. Direção: Carl Gierstorfer, Sebastian Weis. Roteiro: Carl Gierstorfer. Produção: The Why Foundation. Dinamarca, 8 mar. 2018. (58 min.) Disponível em: https://www.thewhy.dk/films/north-koreas-secret-slaves-dollar-heroes. Acesso em: 21 dez. 2024.

North Korea's nuclear program: A history. S.d. Disponível em: https://kls.law.columbia.edu/content/north-koreas-nuclear-program-history. Acesso em: 9 jan. 2025.

NOVETTA Threat Research Group. **Operation Blockbuster**: Unraveling the Long Thread of the Sony Attack. 24 fev. 2016.

NYE Jr., Joseph S. **O Futuro do Poder**. Tradução: Maura Lopes. 1 ed. São Paulo, SP: Benvirá, 2011.

O'NEILL, Patrick Howell. Why was North Korea running a phantom cybersecurity startup in Malaysia? **Cyberscoop**. 27 mar. 2017. Disponível em: https://cyberscoop.com/north-korea-cybersecurity-united-nations-adnet-international/. Acesso em: 27 nov. 2024.

O'REILLY, Tim. **What Is Web 2.0**: Design patterns and business models for the next generation of software. 30 set 2005. Disponível em: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html. Acesso em: 4 mar. 2020.

OLIVEIRA, M. M. **Como fazer pesquisa qualitativa**. Petrópolis: Vozes. 2007.

Organização das Nações Unidas (ONU). **Security Council Committee established pursuant to resolution 1718 (2006)**. United Nations, Security Council, s.d. Disponível em: https://main.un.org/securitycouncil/en/sanctions/1718. Acesso em 13 jan. 2025

_____. **Carta das Nações Unidas**. São Francisco: 26 jun. 1945. Disponível em: https://brasil.un.org/sites/default/files/2022-05/Carta-ONU.pdf. Acesso em: 1º out. 2024.

_____. **Report of the Working Group on Internet Governance**. Château de Bossey, jun. 2005.

_____. **S/RES/1695: Security Council resolution 1695 (2006) [on the launching of ballistic missiles by the Democratic People's Republic of Korea (DPRK)]**. Conselho de Segurança da ONU, 15 jul. 2006a.

_____. **S/RES/1718: Establishment of a Security Council Sanctions Committee (1718 Committee). Imposition of an arms embargo, assets freeze and travel ban on persons involved in the DPRK's nuclear programme, and a ban on a range of imports and exports, to prohibit the DPRK from conducting nuclear tests or launching ballistic missiles**. Conselho de Segurança da ONU, 14 out. 2006b.

_____. **S/RES/1874: Expands measures related to arms' exports and imports to all arms and related material (except import of small arms and light weapons and their related materiel). Calls upon Member States to prevent provision of financial services or transfer of financial resources that could contribute to prohibited programmes/activities.**

States to report on inspections, seizures and disposals, as well as the sale, supply or transfer of small arms or light weapons, among others. Establishes a Panel of Experts, consisting of seven members to assist the 1718 Committee. Conselho de Segurança da ONU, 12 jun. 2009.

_____. **S/2018/171: Report of the Panel of Experts established pursuant to resolution 1874 (2009)**. Conselho de Segurança da ONU, 1 fev. 2018.

_____. **S/2019/171: Report of the Panel of Experts established pursuant to resolution 1874 (2009)**. Conselho de Segurança da ONU, 5 mar. 2019a.

_____. **A/C.3/74/L.11/Rev.1: Countering the use of information and communications technologies for criminal purposes**. Terceiro Comitê da Assembleia Geral da ONU, 5 nov. 2019b.

_____. **S/2024/215: Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)**. Conselho de Segurança da ONU, 7 mar. 2024a.

_____. **A/79/460: Countering the use of information and communications technologies for criminal purposes**: Report of the Third Committee. Terceiro Comitê da Assembleia Geral da ONU, Nova Iorque, NY, EUA, 27 nov. 2024b.

_____. **UN General Assembly adopts landmark convention on cybercrime**. UNODC Press Release. https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html. Acesso em 1 fev. 2025.

OSBORNE, Sherry. **The Number 4 in Korean Culture**. 30 mar. 2023. Disponível em: https://sherryosborne.com/the-number-4-in-korean-culture/. Acesso em: 10 jan. 2025.

PACHECO-PARDO, Ramon. Dandong and Sinuiju: The Sino-North Korean Border Shadow Economy. In: SIMONA, Leila; CLARKSON, Alexander; PACHECO-PARDO, Ramon (eds.). **Dirty Cities**: Towards a Political Economy of the Underground in Global Cities. 1 ed., cap. 4, pp. 89-109. Palgrave-McMillan, 2013.

PAGANINI, P. Russian national arrested in Argentina for laundering money of crooks and Lazarus APT. **Security Affairs**, 24 ago. 2024. Disponível em: https://securityaffairs.com/167485/cyber-crime/russian-national-arrested-laundering-lazarus-funds.html. Acesso em: 9 jan. 2025.

PALACÍN, Valentina. **Practical Threat Intelligence and Data-Driven Threat Hunting**: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools. Birmingham: Packt Publishing, fev. 2021.

PARK, Ju-Min; PEARSON, James. Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West. **Reuters**. 22 mai. 2017. Disponível em: https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020/. Acesso em: 27 nov. 2024.

PATERNOSTER, T. Danos em cabos submarinos foram “sabotagem”, afirma o ministro da defesa alemão. **Euronews**, 19 nov. 2024. Disponível em: https://pt.euronews.com/my-

europe/2024/11/19/danos-em-cabos-submarinos-foram-sabotagem-afirma-o-ministro-da-defesa-alemao. Acesso em: 28 jan. 2025.

PEARSON, James; BING, Christopher. Exclusive: North Korean hackers breached top Russian missile maker. **Reuters**, 7 ago. 2023. Disponível em: https://www.reuters.com/technology/north-korean-hackers-breached-top-russian-missile-maker-2023-08-07/. Acesso em: 17 jun. 2024.

PEREIRA, Iara Xavier. Iara Xavier Pereira (depoimento, 2015). Rio de Janeiro, Centro de Pesquisa e Documentação de História Contemporânea (CPDOC)/Fundação Getúlio Vargas (FGV), 6 h 6 min.

PERL, R. State Crime: The North Korean drug trade. In: **Global crime**, v. 6, n. 1, pp. 117-128, fev. 2004.

PERL, R. **Drug Trafficking and North Korea**: issues for U.S. policy. CRS Report for Congress. 25 jan. 2007.

PERLROTH, Nicole. Report says cyberattacks originated inside Iran. **The New York Times**, 3 dez. 2014. Disponível em: https://www.nytimes.com/2014/12/03/world/middleeast/report-says-cyberattacks-originated-inside-iran.html. Acesso em: 9 mar. 2024.

_____. Cyberattack Caused Olympic Opening Ceremony Disruption. **The New York Times**, 12 fev. 2018. Disponível em: https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html. Acesso em: 19 jan. 2019.

PERLROTH, Nicole; SANGER, David E. North Korea loses its link to the internet. **The New York Times**, 22 dez. 2014. Disponível em: https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html. Acesso em: 19 jan. 2025.

PETERSON, L. L.; DAVIE, B. S. **Computer networks**: A systems approach. 6 ed., Oxford, Reino Unido: Morgan Kaufmann, 2021.

PLATTE, James E. Toward a Joint US-ROK Cyber Deterrence Strategy. **38 North**. 30 nov. 2021. Disponível em: https://www.38north.org/2021/11/toward-a-joint-us-rok-cyber-deterrence-strategy/. Acesso em: 9 mar. 2024.

PRIVACY INTERNATIONAL. **An overbroad, unbalanced and dangerous UN cybercrime treaty must be rejected**. 7 ago. 2024. Disponível em: https://privacyinternational.org/advocacy/5354/overbroad-unbalanced-and-dangerous-un-cybercrime-treaty-must-be-rejected. Acesso em: 2 fev. 2025.

PROPAGANDA Game, The. Direção: Álvaro Longoria, Produção: Álvaro Longoria (Morena Filmes). Espanha/França, 2015. Sob demanda. (98 min.)

RÁDIO NOVELO APRESENTA. 15 minutos de fama. **Rádio Novelo**, 18 mai. 2023. Podcast. Disponível em: https://radionovelo.com.br/originais/apresenta/15-minutos-de-fama/. Acesso em: 21 dez. 2024.

RAMANI, Samuel. The North Korean-Syrian Partnership: Bright Prospects Ahead. **38 North**, 23 mar. 2021. Disponível em: https://www.38north.org/2021/03/the-north-korean-syrian-partnership-bright-prospects-ahead/. Acesso em: 12 jun. 2024.

RECORDED FUTURE. **North Korea Cyber Activity**. Report. 15 jun. 2017. Disponível em: https://www.recordedfuture.com/research/north-korea-cyber-activity. Acesso em: 10 jan. 2025.

_____. **North Korea Cyber Strategy**. Report. 23 jun. 2023. Disponível em: https://www.recordedfuture.com/research/north-koreas-cyber-strategy. Acesso em: 10 jan. 2025.

Rede Nacional de Ensino e Pesquisa (RNP). **Nossa história**. 2019. Disponível em: https://www.rnp.br/sobre-nos/nossa-historia. Acesso em: 14 jun. 2024.

REED, Thomas C. **At the Abyss**: An Insider's History of the Cold War. Nova Iorque, NY, EUA: Ballantine Books, 2004.

RICHARD, Laurent; RIGAUD, Sandrine. **Pegasus**: The story of the most dangerous spyware. Dublin: McMillan Books. 2023.

RICUPERO, Rubens. **A diplomacia na construção do Brasil**: 1750-2016. 1 ed., Rio de Janeiro: Versal, 2017.

RID, T. **Cyber war will not take place**. Oxford, Reino Unido: Oxford University Press, 2017.

_____. **Active measures**: The secret history of disinformation and political warfare. Nova Iorque, NY, EUA: Farrar, Straus and Giroux, 2020.

RID, T.; BUCHANAN, B. **Attributing Cyber Attacks**. The Journal of Strategic Studies, vol. 38, n. 1-2, pp. 4-37. Taylor & Francis, 2015.

ROI, Michael; LYON, Peter. Military Influence Mechanisms. In: FONG, Brian C.H.; CHONG, Ja Ian. **Routledge Handbook of Great Power Competition**. Abingdon, Reino Unido: Routledge, 2025.

SAKELLARIADIS, J. To stem North Korea's missiles program, White House looks to its hackers. **Politico**, 22 dez. 2023. Disponível em: https://www.politico.com/news/2023/12/21/north-korea-missiles-program-hackers-00132871. Acesso em: 24 jun. 2024.

SANGER, D. E. **The perfect weapon**: War, sabotage, and fear in the Cyber Age. Nova Iorque, NY, EUA: Crown, 2018.

SANGER, D. E.; BROAD, W. J. Trump inherits a secret cyberwar against north Korean missiles. **The New York Times**, 4 mar. 2017. Disponível em: https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html. Acesso em: 21 abr. 2024.

SANGER, D. E.; KIRKPATRICK, D. D.; PERLROTH, N. The world once laughed at North Korean cyberpower. No more. **The New York Times**, 15 out. 2017. Disponível em: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html. Acesso em: 21 abr. 2024.

SANG-HUN, Choe. South Korea says it misidentified source of cyberattack. **The New York Times**, 22 mar. 2013. Disponível em: https://www.nytimes.com/2013/03/23/world/asia/south-korea-says-it-misidentified-source-of-cyberattack.html. Acesso em: 29 jan. 2025.

_____. North Korea Tried to Jam GPS Signals Across Border, South Korea Says. **The New York Times**. 1 abr. 2016. Disponível em: https://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html. Acesso em: 19 dez. 2024.

SÁ-SILVA, Jackson Ronie; ALMEIDA, Cristóvão Domingos de; GUIDANI, Joel Felipe. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, ano 1, n. 1, jul. 2009.

SÁVIO, M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação (Mestrado em Engenharia de Sistemas e Computação), Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

SCHMITT, Michael N. (ed. gen.) **Tallinn manual 2.0 on the international law applicable to cyber operations**: prepared by the International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence. 2 ed. Cambridge, Reino Unido: Cambridge University Press, 2017.

SCHNEIER, Bruce. **Click Here to Kill Everybody**: Security and Survival in a Hyper-connected World. Nova Iorque, NY, EUA: W.W. Norton & Company, 2018.

SECURITY COUNCIL REPORT. **U.N. Sanctions**. Special Research Report, n. 3, 25 nov. 2015. Disponível em: http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/special_research_report_sanctions_2013.pdf. Acesso em: 4 nov. 2024.

SEGAL, Adam. **The hacked world order**: how nations fight, trade, maneuver, and manipulate in the digital age. 2 ed., Nova Iorque, NY, EUA: PublicAffairs, 2017.

SELIGER, Bernhard; SCHMIDT, Stefan. The hermit kingdom goes online: Information Technology, Internet use and communication policy in North Korea. **North Korean Review**, v. 10, n. 1, p. 71–88, 2014.

SEO, Y.; REGAN, H. North Korean factories making arms for Russia are 'operating at full capacity,' South Korea says. **CNN**, 28 fev. 2024. Disponível em: https://edition.cnn.com/2024/02/28/asia/north-korea-munitions-factories-shipments-russia-ukraine-intl-hnk/index.html. Acesso em: 23 jun. 2024.

SETH, M. J. **A Concise History of Korea**: From Antiquity to the Present. 3 ed., Lanham, MD: Rowman & Littlefield, 2020.

_____. From hermit kingdom to colony. In: **Asia in World History: 1750-1914**, v. 13, n. 2, pp. 28-33, 2008. Disponível em: https://www.asianstudies.org/wp-content/uploads/korea-from-hermit-kingdom-to-colony.pdf. Acesso em: 5 jun. 2024.

SEUNG-WOO, Kang. North Korea increases cyberattacks on South Korea. **The Korea Times**. 1 jul. 2021. Disponível em:

https://www.koreatimes.co.kr/www/nation/2021/07/103_311462.html. Acesso em: 29 jan. 2025.

SHAIKH, Asseem. 'Cosmos Bank cloned card heist planned in Thane'. **The Times of India**. 12 dez. 2018. Disponível em: https://timesofindia.indiatimes.com/city/mumbai/cosmos-bank-cloned-card-heist-planned-in-thane/articleshow/67051609.cms. Acesso em: 29 jan. 2025.

SHARMA, Abhishek. **North Korea's Cyber Strategy**: An Initial Analysis. Issue Brief no. 755. Nova Delhi, Índia: Observer Research Foundation, nov. 2024.

SHELLEY, L. I. **Dark commerce**: How a new illicit economy is threatening our future. Princeton, EUA: Princeton University Press, 2020.

SIEBRA, Eduardo Figueiredo, Aspectos Estratégicos das Relações entre Brasil e Coreia do Norte in BARBOSA, Paulo Henrique Batista (ed.), **Os Desafios e Oportunidades na Relação Brasil-Asia na Perspectiva de Jovens Diplomatas**. Cap. 6, pp. 201-238, Brasília: FUNAG, 2017.

SIMOES, Alexander JG; HIDALGO, César A. The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development. In: **Proceedings of the 17th AAAI Conference – Workshop on Scalable Integration of Analytics and Visualization**, pp. 39-42, 2011.

SMITH, Josh. N. Korean Internet downed by suspected cyber attacks - researchers. **Reuters**, 26 jan. 2022. Disponível em: https://www.reuters.com/world/asia-pacific/nkorean-internet-downed-by-suspected-cyber-attacks-researchers-2022-01-26/. Acesso em: 7 mar. 2024.

SOLDATOV, Andrei; BOROGAN, Irina. **Russian Cyberwarfare**: Unpacking the Kremlin's Capabilities. Center for European Policy Analysis (CEPA), 8 set. 2022. Disponível em: https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/. Acesso em: 22 jun. 2024.

SOLOMON, Jay; CHI, Hae Won. In North Korea, secret hoard of cash props up a regime. **The Wall Street Journal**, p. A1, 14 jul. 2003.

SOUZA, Marcos de Moura e; BRAUN, Daniela. Brasileiro que comanda combate ao cibercrime na Interpol revela quem está por trás e o que motiva o sequestro de dados. **Valor Econômico**, 26 dez. 2024. Disponível em: https://valor.globo.com/empresas/noticia/2024/12/26/cibercrime-avanca-sobre-infraestrutura-critica-diz-interpol.ghtml. Acesso em: 26 dez. 2024.

STAHLER, Kevin; HAGGARD, Stephan. More Cyber: The Korea Hydro and Nuclear Power Company (KHNP) Hacks. **Peterson Institute for International Economics (PIIE) blogs**. 13 fev. 2013. Disponível em: https://www.piie.com/blogs/north-korea-witness-transformation/more-cyber-korea-hydro-and-nuclear-power-company-khnp. Acesso em: 27 jan. 2025.

STEVENSON, Alastair. Iran and North Korea sign technology treaty to combat hostile malware. **V3.co.uk**, 3 set. 2012. Disponível em: https://web.archive.org/web/20120906211943/http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware. Acesso em: 26 dez. 2024.

STOLL, Clifford. **The Cuckoo's Egg**: Tracking a Spy Through the Maze of Computer Espionage. Doubleday, 1989.

STUBBS, Jack. Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources. **Reuters**. 27 nov. 2020. Disponível em: https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSKBN2871A2/. Acesso em: 27 nov. 2024.

STUCKEY, Daniel; BLAKE, Andrew. Exclusive: How FBI informant Sabu helped anonymous hack Brazil. **Vice**. 5 jun. 2014. Disponível em: https://www.vice.com/en/article/exclusive-how-an-fbi-informant-helped-anonymous-hack-brazil/. Acesso em: 28 jan. 2025.

SUTTON, H. I. Russia's suspected internet cable spy ship vanishes off the Americas. **Forbes**. Disponível em: https://www.forbes.com/sites/hisutton/2019/11/19/russias-suspected-internet-cable-spy-ship-vanishes-off-the-americas/. Acesso em: 13 jan. 2025.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. **Computer networks**, 6 ed., Londres, Reino Unido: Pearson Education, 2021.

TERRY, S. M. North Korea's nuclear family: How the Kims Got the Bomb and Why They Won't Give It Up. **Foreign Affairs**, 24 ago. 2021.

TERTITSKIY, Fyodor. Why is North Korea sending troops to fight for Russia? **Carnegie Endowment for International Peace**. 7 nov. 2024. Disponível em: https://carnegieendowment.org/russia-eurasia/politika/2024/11/russia-north-korea-new-allies?lang=en. Acesso em: 4 dez. 2024.

THAICERT. **Threat Group Cards**: A threat actor encyclopedia, version 2.0. 8 jul. 2020. Disponível em: https://apt.etda.or.th/img/Threat_Group_Cards_v2.0.pdf. Acesso em: 17 jun. 2024.

_____. **APT group: Lazarus Group, Hidden Cobra, Labyrinth Chollima**. 29 dez. 2024. Disponível em: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima. Acesso em: 10 jan. 2025.

THOMAS, T. L. **Cyber silhouettes**: Shadows over information operations. Foreign Military Studies Office, 25 mai. 2005.

_____. Information security thinking: A comparison of U.S., Russian, and Chinese concepts. In: **International Seminar on Nuclear War and Planetary Emergencies**. World Scientific, pp. 344-358, ago. 2001.

TIDMARSH, David. **Diamond Model of Intrusion Analysis: What, Why, and How to Learn**. 7 nov. 2023. Disponível em: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/. Acesso em: 27 jan. 2025.

TJIA, Paul. North Korea: An Up-and-Coming IT-Outsourcing Destination. **38 North**, 26 out. 2011. Disponível em: https://www.38north.org/2011/10/ptjia102611/. Acesso em: 8 dez. 2024.

TRMLABS. Tornado cash volume dramatically reduced post sanctions, but illicit actors are still using the mixer. **TRM Blog**, 11 out. 2023. Disponível em: https://www.trmlabs.com/post/tornado-cash-volume-dramatically-reduced-post-sanctions-but-illicit-actors-are-still-using-the-mixer. Acesso em: 30 jan. 2025.

TROPINA, Tatiana. Cybercrime: setting international standards. In: TIKK E. & KERTUNEN M. (eds.), **Handbook of International Cybersecurity**. Cap. 11, pp. 148-160, Abingdon, Reino Unido: Routledge, 2020.

TURTON, W. A US company enabled a north Korean scam that raised money for WMDs. **Wired**, 5 jun. 2024. Disponível em: https://www.wired.com/story/registered-agents-north-korean-scam-wmds/. Acesso em: 24 jun. 2024.

UNGOED-THOMAS, Jonathan. How 'Datastream Cowboy' Took U.S. to the Brink of War, **Toronto Star**, 1º jan. 1998.

URBINA, I. Inside North Korea's forced-labor program in China. **New Yorker**, n. 1925. 25 fev. 2024.

UREN, Tom. The Three I's In Spyware. **Lawfare**, 13 set. 2024. Disponível em: https://www.lawfaremedia.org/article/the-three-i's-in-spyware. Acesso em: 5 fev. 2025.

VALERIANO, Brandon; JENSEN, Benjamin; MANESS, Ryan C. **Cyber Strategy**: The evolving character of power and coercion. Nova Iorque, NY, EUA: Oxford University Press, 2018.

VAN PUYVELDE, D.; BRANTLY, A. **Cybersecurity**: Politics, Governance and Conflict in Cyberspace. Cambridge, Reino Unido: Polity Press, 2019.

VOO, Julia; HEMANI, Irfan; JONES, Simon. **National Cyber Power Index 2022**. Cambridge, MA: Harvard Kennedy School, set. 2022.

WALK FREE. **The Global Slavery Index 2023**. 2023

WALTZ, Kenneth N. **Theory of International Politics**. Addison-Wesley, 1979.

WARNER, M. Cybersecurity: A pre-history. **Intelligence & National Security**, v. 27, n. 5, p. 781-799, 2012.

WAZLAWICK, Raul Sidnei. **História da Computação**. 1 ed., Rio de Janeiro: Elsevier, 2016.

WEBER, Max. **Ciência e Política**: duas vocações (trad.). São Paulo: Cultrix, 2011.

WEIMANN, Gabriel. **Terror on the Internet**: the new arena, the new challenges. Washington, DC, EUA: United States Institute of Peace, 2006.

WHITE, Geoff. **Crime dot com**: From viruses to vote rigging, how hacking went global. Reaktion Books Ltd., 2020.

_____. **The Lazarus Heist**: From Hollywood to High Finance: Inside North Korea's Global Cyber War. Penguin Books, 2022.

_____. **Rinsed**: From Cartels to Crypto: How the Tech Industry Washes Money for the World's Deadliest Crooks. Penguin Books, 2024.

WIENER, Norbert. **Cybernetics**: or the Control and Communication in the Animal and the Machine. 2 ed. (reedição), Cambridge, MA, EUA: MIT Press, 2019.

WILLIAMS, Martyn. Exclusive: North Korea's Samjiyon tablet – Made in China? **38 North**, 4 ago. 2013. Disponível em: https://www.northkoreatech.org/2013/08/04/exclusive-north-koreas-samjiyon-tablet-made-in-china/. Acesso em: 8 dez. 2024.

_____. How the internet works ("works") in North Korea. **Slate**, 28 nov. 2016. Disponível em: https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html. Acesso em: 23 jun. 2024.

_____. All That Glitters Is Not Gold: A Closer Look at North Korea's Ullim Tablet. **North Korea Tech**, 3 mar. 2017. Disponível em: https://www.38north.org/2017/03/mwilliams030317/. Acesso em: 8 dez. 2024.

_____. North Korea's Kangsong is operating a 4G network. **North Korea Tech**, 7 mar. 2024a. Disponível em: https://www.northkoreatech.org/2024/03/07/north-koreas-kangsong-is-operating-a-4g-network/. Acesso em: 8 dez. 2024.

WOHLFORTH, William C. Realism. In: REUS-SMITH, Christian; SNIDAL, Duncan. (eds.) **The Oxford Handbook of International Relations**. Oxford, Reino Unido: Oxford University Press, 2008.

WYLER, Liana Sun; NANTO, Dick K. **North Korean Crime-for-Profit Activities**. CRS Report for Congress. Washington, DC, EUA: CRS, 25 ago. 2008.

XU, Tianran. Surpass the Cutting Edge: Reflections on North Korea's Failed May 27 Satellite Launch. **38 North**. 7 jun. 2024. Disponível em: https://www.38north.org/2024/06/surpass-the-cutting-edge-reflections-on-north-koreas-failed-may-27-satellite-launch/. Acesso em: 19 jan. 2025.

YADAV, Tarun; RAO, Arvind Mallari. Technical Aspects of Cyber Kill Chain. In: Conference: In: ABAWAJY, J. H. *et al.* (eds.), **Security in computing and communications**: Third International Symposium on Security in Computing and Communications (Proceedings), pp. 438-452. Springer International Publishing, 10-13 ago. 2015.

YIN, Robert. K. **Estudo de caso**: Planejamento e métodos. 2 ed., Porto Alegre: Bookman, 2001.

YOON, S. North Korea recruits hackers at school. **Al Jazeera**, 20 jun. 2011. Disponível em: https://www.aljazeera.com/features/2011/6/20/north-korea-recruits-hackers-at-school. Acesso em: 23 jun. 2024.

ZETTER, K. Cybersleuths uncover 5-year spy operation targeting governments, others. **Wired**, 14 jan. 2013. Disponível em: https://www.wired.com/2013/01/red-october-spy-campaign/. Acesso em 29 jan. 2025.

_____. **Countdown to zero day**: Stuxnet and the launch of the world's first digital weapon. Nova Iorque, NY, EUA: Broadway Books, 2014.

APÊNDICE A Informações técnicas sobre a família de protocolos TCP/IP

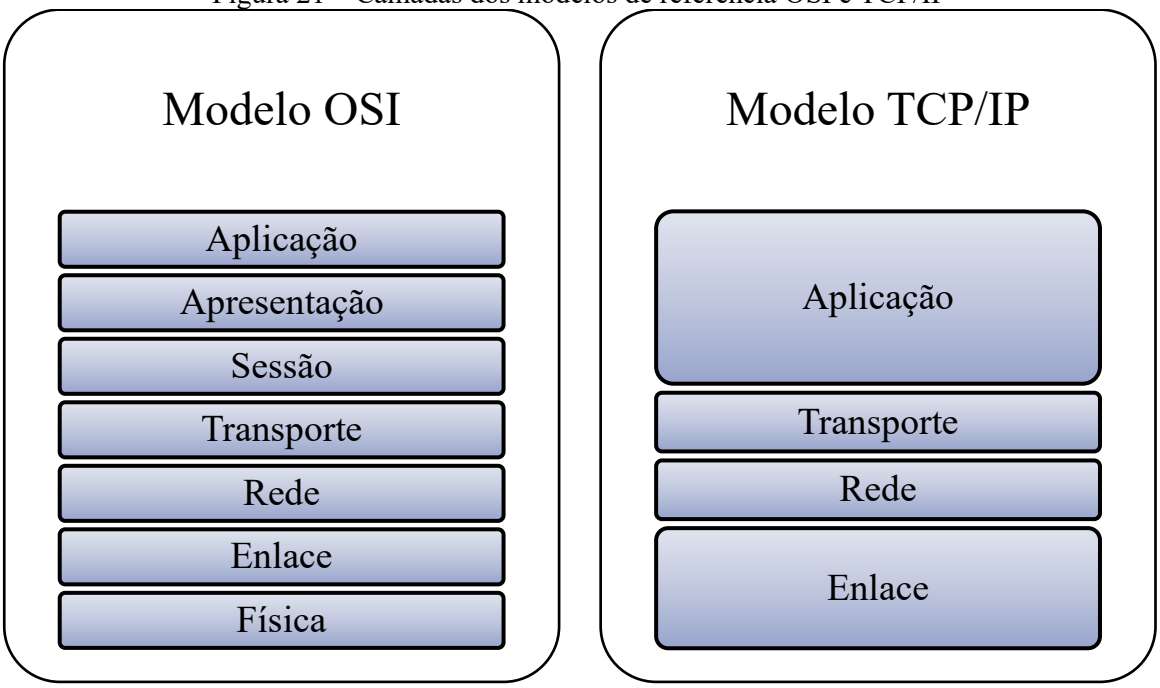
Este apêndice contém informações básicas sobre modelos de referência e famílias de protocolos, com um pouco mais de detalhes quanto aos protocolos TCP/IP. Não é uma referência completa sobre o assunto, mas uma fonte para ampliar o conhecimento de quem não é familiar à área de sistemas computacionais ou redes de computadores. Pelo mesmo motivo, não traz informações técnicas aprofundadas.

Na década de 1960, houve diversas experiências com redes de comunicação utilizando comutação de pacotes (*packet switching*) em contraponto à comutação de circuitos (*circuit switching*). A família de protocolos TCP/IP, do tipo comutação de pacotes, foi uma dessas experiências, não a única, mas a que obteve mais sucesso. Os protocolos desse tipo de rede foram construídos separados em camadas, cada uma abstraindo os serviços que proviam. O modelo de referência mais comum é o criado pela ISO chamado de *Open Systems Interconnection* (OSI) (TANENBAUM *et al.*, 2021, pp. 59-64). O modelo OSI é dividido em sete camadas: aplicação, apresentação, sessão, transporte, interconexão, enlace e físico[178]. Empilhados nessa ordem, cada camada oferece serviços à camada superior e requisita outros à inferior. E a camada física, como se pode presumir pelo nome, é responsável pelo serviço de interagir com algum meio físico para que ocorra a comunicação, como por exemplo um cabo de cobre, pares de fios, ondas eletromagnéticas ou fibras óticas.

O modelo de referência TCP/IP e sua família de protocolos podem ser considerados uma simplificação do modelo OSI, dado que não possuem as camadas de apresentação e sessão, com suas funcionalidades, quando necessárias, assumidas pela camada de aplicação, e a camada de enlace. Com este modelo de referência, foram criados os protocolos de comunicação de cada camada, dois dos quais deram nome ao modelo: o *Transport Control Protocolo* (TCP), da camada de transporte, e o *Internet Protocol* (IP), da camada de rede. A Figura 21 apresenta, visualmente, as camadas de cada um dos modelos aqui listados.

[178] Seus nomes, originalmente em inglês, são: *application*, *presentation*, *session*, *transport*, *network*, *link* e *physical*.

Figura 21 – Camadas dos modelos de referência OSI e TCP/IP



Fonte: elaboração própria.

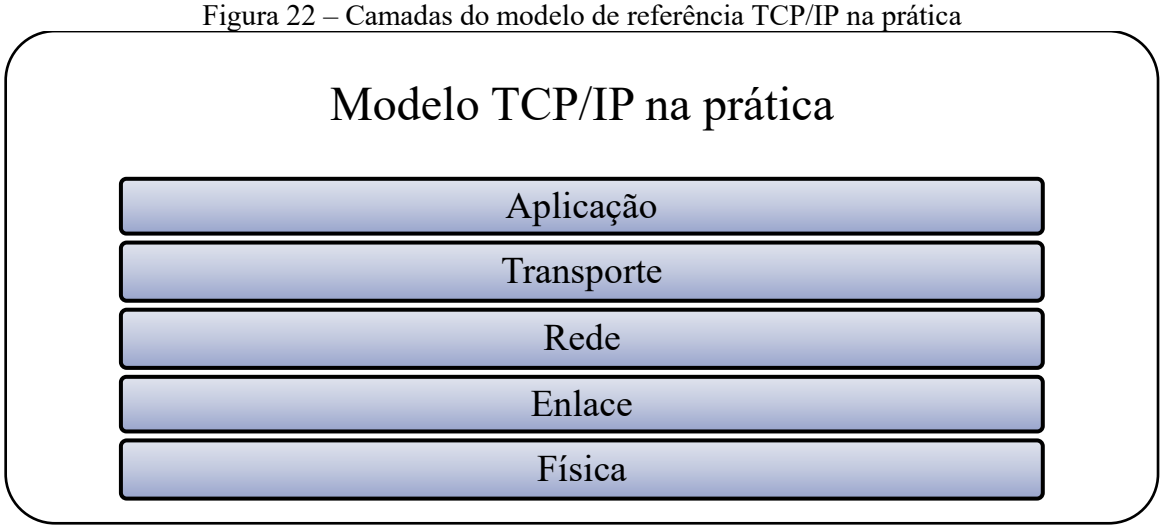
Conforme dito, cada camada dos modelos oferece serviços à camada superior. E cada camada possui um ou mais protocolos a ela associados. Pensando num dispositivo computacional, essa pilha de protocolos é implementada no seu sistema operacional. Como os protocolos são padrão, não interessa o tipo de equipamento ou sistema operacional. Caso a pilha de protocolos TCP/IP esteja implementada em ambos, a comunicação é possível entre as camadas similares. Ou seja, a camada de transporte de um equipamento A é capaz de se comunicar com a mesma camada de um equipamento B, e vice-versa.

Uma camada que destaco é a de Rede, pela seguinte razão: é nela que se coloca a identificação do equipamento na rede, chamado de endereço. Este endereço não se encontra na forma de nomes de rua, avenida, alameda... Os endereços são representados em bits[179] e bytes[180], unidades com as quais um computador é capaz de lidar. Esta camada também determina a forma de encaminhamento de pacotes a outros equipamentos. Este encaminhamento é feito com base no endereço de destino e com base no que chamamos de *tabelas de roteamento*.

[179] O *bit*, cuja origem é a expressão em inglês *binary digit* (dígito binário), é a menor unidade utilizada em um sistema computacional, seja para transmissão no caso de redes, quanto para armazenamento. O bit é representado em base 2, ou seja, assume dois valores: 0 ou 1.
[180] O *byte* é uma sequência agrupada de oito bits, também chamada de octeto.

O modelo TCP/IP foi evoluindo na prática e, de forma didática, hoje pode ser considerado o apresentado na Figura 22.

Figura 22 – Camadas do modelo de referência TCP/IP na prática



Fonte: elaboração própria.

Com relação às camadas e protocolos do modelo TCP/IP, podemos exemplificar os seguintes:

- Aplicação: *Hypertext Transfer Protocol* (HTTP), *Hypertext Transfer Protocolo, Secure* (HTTPS);
- Transporte: *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP);
- Rede: *Internet Protocol* (IP);
- Enlace e física: *Ethernet*, *Wi-Fi*.

Conforme dito, como a camada de rede é a responsável pelo endereçamento dos pacotes que trafegam em uma rede, no caso das redes TCP/IP isso se trata de um papel do protocolo IP, daí pode-se ouvir e ler bastante a expressão “endereço IP”. Este endereço, atribuído a todo equipamento conectado a uma rede TCP/IP, no caso do protocolo IPv4 (ou Internet Protocol, versão 4), é formado por uma sequência de 32 bits, ou seja, 4 bytes. Cada endereço, por legibilidade, ao invés de ser representado como uma sequência de 32 bits, é agrupado em octetos, separados por ponto e, para ficar mais fácil para um ser humano ler e falar, convertido para a base decimal (base 10). Assim, o endereço IPv4 11000000101010000000001000000001 pode ser lido e compreendido mais facilmente como 192.168.2.1. Como cada octeto é representado por 8 bits, seus valores variam de 0 a 255, e a totalidade de endereços que o IPv4 permitiria endereçar é de 2^{32} (ou 4.294.967.296) equipamentos. Essa quantidade de equipamentos parece grande, mas quando se trata de uma rede efetivamente mundial, percebeu-

se que essa quantidade de endereços era bastante insuficiente. Se imaginarmos que, na nossa sociedade, é considerado normal uma pessoa ter ao menos um dispositivo computacional (um telefone celular tipo *smartphone*), percebe-se que o espaço de endereçamento possibilitado pelo IPv4 não permitiria dar um endereço para cada cidadão do mundo. Apesar da criação e aplicação de várias soluções para o problema, como por exemplo o compartilhamento de um mesmo endereço IPv4 por vários equipamentos de uma rede, percebeu-se que isso não seria suficiente. Os últimos endereços IPv4 foram alocados em 25 de novembro de 2019 (TANNENBAUM et at., 2021, p. 461) mas, no entanto, a solução para este problema já estava sendo pensada e implantada há anos.

Desde 1990 a IETF já buscava respostas a essa questão de endereçamento, bem como de outros que não são aqui listados, por não apresentarem pertinência ao trabalho[181]. Foi-se, então, adotado o novo protocolo chamado de IPv6 (ou Internet Protocol, versão 6[182]), o qual foi estruturado de forma a permitir seu funcionamento conjuntamente ao IPv4, o que é a atual realidade da Internet: dois protocolos de endereçamento, compatíveis entre si, funcionando simultaneamente.

O IPv6 tem seus endereços utilizando 128 bits, ao contrário dos 32 bits anteriores. Isso permite 2^{128} endereços no total, correspondente a 340.282.366.920.938.463.463.374.607.431.768.211.456 (mais que 340 undecilhões, ou 340 x 10^{36}). Isso seria capaz de endereçar, com folga, cada milímetro quadrado da Terra (que são $\approx 5{,}101 \times 10^{20}$ mm²). Claro que esse não é o objetivo desse imenso espaço de endereçamento. Em 2011 um artigo relacionado com a "Internet das Coisas" (em inglês *Internet of Things*, IoT), elaborado pela empresa Cisco, estima que por volta de 2008 e 2009 passou-se a ter mais dispositivos e equipamentos conectados à Internet do que pessoas (EVANS, 2011, p. 3). Ou seja, a ampliação do endereçamento seria importante para uma nova família de dispositivos computacionais (da IoT) que necessitava dessa conectividade.

Sobre o endereço anteriormente exemplificado (192.168.2.1), utilizando um endereçamento IPv6 compatível com o IPv4, utilizando todos os 128 bits, seria: 00000000000000000000000000000000000000000000000011111111111111110000000110010010000000010110100000000000000000010000000000000001 ou, usando a nova notação

[181] Tanenbaum *et al.* (2021, pp. 462-463) listam os problemas relacionados ao IPv4, bem como Peterson e Davie (2022, pp. 309-310).

[182] A mudança de um protocolo versão 4 para outro versão 6 é porque houve um protocolo experimental, representado pelo número 5, anos antes e que não foi oficialmente adotado (PETERSON e DAVIE, 2022, p. 309).

que foi adotada, utilizando base 16 e números hexadecimais[183]: 0000:0000:0000:ffff:0192:0168:0002:0001. Para simplificação, substituem-se sequências de zeros por "::" . O endereço se torna, então, ::ffff:192:168:2:1.

Entretanto, na realidade, a quantidade possível de endereços não é exatamente a descrita acima, isso porque alguns endereços são reservados para usos específicos e, ainda, não faz sentido endereços contíguos, como 192.168.2.1 e 192.168.2.2, terem rotas de destinação distintas[184]. Os endereços são, portanto, agregados e distribuídos em conjuntos como, por exemplo, os endereços de 192.168.2.0 até 192.168.2.255 estarem alocados numa mesma rede de computadores. O tratamento dado pelas tabelas de roteamento também fica simplificado, tendo em vista que, neste caso, bastaria analisar os 3 primeiros octetos (ou 24 primeiros bits) para se determinar se um endereço estaria dentro desta rede. Ainda, dentro dessa rede de exemplo, dois endereços não podem ser utilizados: 192.168.2.0 e 192.168.2.255. Em termos técnicos, eles representam o prefixo da rede e seu endereço de *broadcast*. É como se o primeiro representasse uma rua, e os endereços intermediários (de 1 a 254) representassem cada uma das casas ali existentes (os equipamentos conectados à rede). O segundo endereço, *broadcast*, é utilizado para indicar que um certo pacote deve ser encaminhado e lido por todas as casas da rua, e não somente uma específica[185]. Essa observação é aqui posta só para mostrar que, ao final, a quantidade de endereços IPv4 é, na verdade, bem menor que os 4.294.967.296 possíveis, já que cada rede conectada tem ao menos esses dois endereços especiais que devem ser retirados desse cálculo. Além destes, há endereços especiais reservados[186] para usos especiais que não são de relevância para este trabalho, mas que reduzem ainda mais a quantidade de equipamentos possíveis de serem endereçados.

[183] Na base 16, cada dígito pode assumir 16 valores, os quais são representados de 0 a 9 e de A a F.
[184] O exemplo aqui é para endereços IPv4, mas nisso o IPv6 apresenta questões semelhantes.
[185] Para informações e explicações mais completas, sugiro Tanenbaum *et al.* (2021, pp. 448-456) e Peterson e Davie (2022, pp. 211-219).
[186] A lista de endereços IP reservados é mantida pela IANA e está disponível em: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtm.

ANEXO A Conteúdo da Seção 1 - Direito Penal da Convenção de Budapeste, conforme internalizado pelo Decreto nº 11.417

Seção 1 - Direito Penal
Título 1 - Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador

Artigo 2 - Acesso ilegal
Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador.

Artigo 3 - Interceptação ilícita
Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões eletromagnéticas oriundas de um sistema informatizado que contenham esses dados de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com objetivo fraudulento ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador.

Artigo 4 - Violação de dados
1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a danificação, a eliminação, a deterioração, a alteração ou a supressão dolosas e não autorizadas de dados de computador.

2. Qualquer Parte pode reservar-se o direito de exigir que da conduta descrita no parágrafo 1 resulte sério dano para a vítima.

Artigo 5 - Interferência em sistema
Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crime, em sua legislação interna, qualquer grave obstrução ou impedimento, dolosos e não autorizados, do funcionamento de um sistema de computador por meio da inserção, transmissão, danificação, apagamento, deterioração, alteração ou supressão de dados de computador.

Artigo 6 - Uso indevido de aparelhagem
1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:
a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:
i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;
ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e
b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize.

2. Este Artigo não deve ser interpretado para estabelecer responsabilidade criminal quando a produção, venda, aquisição para uso, importação, distribuição ou disponibilização por qualquer meio ou a posse referidos no parágrafo 1 deste Artigo não se destine à prática de qualquer dos crimes tipificados de acordo com os artigos 2 a 5 desta Convenção, como para, por exemplo, a realização de testes autorizados ou a proteção de um sistema de computador.

3. Cada Parte pode reservar-se o direito de não aplicar o parágrafo 1 deste Artigo, desde que a reserva não se refira à venda, distribuição ou a disponibilização por qualquer meio, dos itens ou instrumentos referidos no parágrafo 1 a.ii deste Artigo.

Título 2 - Crimes informáticos
Artigo 7 - Falsificação informática

Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador, de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento.

Artigo 8 - Fraude informática
Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:

a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;
b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita.

Título 3 - Crimes relacionados ao conteúdo da informação
Artigo 9 - Pornografia infantil

1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando cometidas dolosamente e de forma não autorizadas:
a. produzir pornografia infantil para distribuição por meio de um sistema de computador;
b. oferecer ou disponibilizar pornografia infantil por meio de um sistema de computador;
c. distribuir ou transmitir pornografia infantil por meio de um sistema de computador;
d. adquirir, para si ou para outrem, pornografia infantil por meio de um sistema de computador;
e. possuir pornografia infantil num sistema de computador ou num dispositivo de armazenamento de dados de computador.

2. Para os fins do parágrafo 1, "pornografia infantil" inclui material pornográfico que represente visualmente:
a. um menor envolvido em conduta sexual explícita;
b. uma pessoa que pareça menor envolvida em conduta sexual explícita;
c. imagens realísticas retratando um menor envolvido em conduta sexual explícita.

3. Para os fins do parágrafo 2, o termo "menor" inclui todas as pessoas com menos de 18 anos de idade. Qualquer Parte pode, contudo, estabelecer um limite de idade diverso, que não será inferior a 16 anos.

4. Qualquer Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o parágrafo 1, subparágrafos d e e, e o parágrafo 2, subparágrafos b e c.

Título 4 - Violação de direitos autorais e de direitos correlatos
Artigo 10 - Violação de direitos autorais e de direitos correlatos

1. Cada Parte adotará medidas legislativas semelhantes e outras providências necessárias para tipificar como crimes, em sua legislação interna, a violação de direitos autorais, como definidos no direito local, segundo as obrigações assumidas sob o Ato de Paris, de 24 de julho de 1971, que modificou a Convenção de Berna para a Proteção de Obras Literárias e Artísticas, o Acordo sobre Aspectos Comerciais da Propriedade Intelectual e o Tratado de Direitos Autorais da OMPI, com exceção de quaisquer direitos morais conferidos por tais convenções, quando tal conduta violadora for cometida intencionalmente, em escala comercial e por meio de um sistema de computador.

2. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a violação de direitos correlatos aos autorais, como definidos, no direito local, de acordo com as obrigações assumidas em face da Convenção Internacional para a Proteção de Artistas, Produtores de Fonogramas e Organizações Rádio-difusoras, assinada em Roma (Convenção de Roma), o Acordo sobre Aspectos Comerciais da Propriedade Intelectual e o Tratado da OMPI sobre Atuações Artísticas e Fonogramas, com exceção de quaisquer direitos morais conferidos por tais convenções, quando tal conduta violadora for cometida dolosamente, em escala comercial e por meio de um sistema de computador.

3. Qualquer Parte pode reservar-se o direito de não impor responsabilidade criminal no tocante às condutas dos parágrafos 1 e 2 deste Artigo em circunstâncias limitadas, desde que outras soluções jurídicas eficazes estejam disponíveis e que tal reserva não seja estipulada em detrimento das obrigações internacionais do Estado, estabelecidas nos instrumentos internacionais referidos nos parágrafos 1 e 2 deste Artigo. (BRASIL, 2023a)