Guerra Cibernética no contexto das Infraestruturas Críticas

1º Ten João Marcos Barbosa Oliveira*

RESUMO

A proteção das Infraestruturas Críticas (IC) é vital para qualquer nação. Com a evolução de sua gestão dependendo cada vez mais de computação, redes, nuvem, *hardware*, *software* e infraestrutura de TI, a segurança desses ativos tem se tornado uma área crítica e mantê-los seguros talvez seja o aspecto mais importante de sua segurança hoje. Com a finalidade de se obter êxito na sua proteção é necessário conhecer as áreas de IC mais vulneráveis a esse tipo de ataque. Neste contexto, este artigo teve como objetivo identificar quais as áreas de IC que mais sofreram ataques exitosos de Guerra Cibernética. Foi realizada uma pesquisa na literatura disponível sobre o assunto e a partir dos estudos encontrados pôde-se concluir que a área de IC que mais sofreu ataques cibernéticos exitosos é a de Energia. A identificação dessa área serve aos integrantes do Sistema de Guerra Cibernética do Exército (SGCEx) como base para o planejamento de ações de exploração das infraestruturas críticas inimigas.

Palavras-chave: Guerra Cibernética; Ataque Cibernético; Infraestruturas Críticas.

Cyber Warfare in the context of Critical Infrastructures

ABSTRACT

The security of Critical Infrastructure (CI) is vital for any nation. With the evolution of its management as more and more computers, networks, cloud, hardware, software and IT infrastructure, the security of these assets has become a critical area and needing them safely is perhaps the most important aspect of your security today. With this intention, it is necessary to know how areas of CIs are most vulnerable to this type of attack. In this context, this article aimed to identify which CIs suffered the most successful cyber attacks. A research was carried out with the available literature on the subject and according to the studies found it was possible to conclude that the area of CI that suffered the most successful cyber attacks is Energy. The identification of this area serves the members of the Army's Cyber Warfare System as a basis for planning actions to exploit enemy critical infrastructures.

Keywords: Cyber Warfare; Cyber Attack; Critical Infrastructure.

1 INTRODUÇÃO

A Guerra Cibernética pode apresentar uma infinidade de ameaças para uma nação. No nível tático, ataques cibernéticos podem ser usados para apoiar a guerra tradicional. Por exemplo, adulteração do mecanismo operação de defesas aéreas por meios cibernéticos, de modo a facilitar um ataque aéreo (WEINBERGER, 2007). Por outro lado, podem apoiar operações não tão tradicionais, tais como realizar um ataque a uma usina de enriquecimento de urânio (CHEN, 2010) ou até mesmo a sistemas bancários de um país (JENIK, 2009). Além dessas ameaças diretas, a guerra cibernética também pode contribuir para ameaças indiretas, como espionagem e propaganda.

Como em qualquer conflito, a Guerra Cibernética tem sido considerada uma questão significativa na política mundial. No entanto, diferentemente da guerra convencional, a guerra cibernética torna difícil, senão impossível, saber quem é o agressor (EXÉRCITO BRASILEIRO, 2017). Por causa disso, houve uma corrida armamentista para tornar a divisão cibernética totalmente funcional em alguns países, pronta para realizar um ataque cibernético ou defender-se de um.

Os ataques cibernéticos podem ter diferentes categorias de alvos, porém os mais comuns estão englobados no conceito de Infraestruturas Críticas (IC) (CARVALHO, 2011). Essas infraestruturas abrangem instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (MANDARINO JUNIOR, 2010).

Inserido neste contexto e para desenvolvimento desse artigo, foi elaborada a seguinte questão de pesquisa: Quais foram as Áreas de Infraestruturas Críticas que mais sofreram ataques exitosos de Guerra Cibernética? Dessa forma, o objetivo desse artigo foi identificar essas áreas.

Justifica-se essa pesquisa devido ao fato que sua identificação pode servir aos integrantes do Sistema de Guerra Cibernética do Exército (SGCEx) como base para o planejamento de ações

de exploração das Infraestruturas Críticas inimigas e também na coordenação e integração da proteção das IC de interesse para a Defesa Nacional.

2 REFERENCIAL TEÓRICO

Este referencial teórico tem como finalidade apresentar os conceitos sobre Guerra Cibernética, Ataque Cibernético e Áreas de Infraestruturas Críticas, do ponto de vista da literatura acadêmica da área e das definições do Exército Brasileiro e do Gabinete de Segurança Institucional, que foram utilizados como pilares desse artigo.

2.1 GUERRA CIBERNÉTICA

O termo guerra de informação, precursor do atual termo guerra cibernética tem uma história que remonta à década de 70. O primeiro uso registrado do termo foi por Thomas Rona em 1976 (ROBINSON; JONES, 2015). Rona definiu o que ele chamou de guerra de informação como: competições de nível estratégico, operacional e tático em todo o espectro de paz, crise, escalada de crise, conflito, guerra, término de guerra e reconstituição/restauração, travadas entre concorrentes, adversários ou inimigos usando meios de informação para atingir seus objetivos. (RONA, 1976 apud LIBICK, 1995, p. 14).

Um grande número de definições de Guerra Cibernética foi sugerido com o passar dos anos, sem que uma seja amplamente adotada internacionalmente (HATHAWAY *et al*, 2012). Alford (2001, p. 21) definiu a guerra cibernética como:

> qualquer ato destinado a obrigar um oponente a cumprir nossa vontade nacional, executado contra os processos de controle de *software* dentro de um sistema do oponente. (ALFORD, 2001, p. 21).

e Parks e Duggan (2011, p. 123) definem como: "Guerra Cibernética é uma combinação de ataque e defesa de rede de computadores e operações técnicas especiais".

Segundo o Exército Brasileiro (2007) a Guerra Cibernética:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC (EXÉRCITO BRASILEIRO, 2017, p. 18).

O conceito de Comando e Controle (C2) é importante para o entendimento que o Exército Brasileiro tem sobre Guerra Cibernética. Segundo o Glossário das Forças Armadas (2015, p. 65) C2 é "Ciência e arte que trata do funcionamento de uma cadeia de comando". Ora, a Guerra Cibernética, então, nesse contexto, procura atingir o exercício da autoridade e da direção que um comandante tem sobre as forças sob o próprio comando.

2.2 ATAQUE CIBERNÉTICO

Desde o final dos anos de 1970, os ataques cibernéticos desenvolveram-se para tornar ferramentas de tecnologia da informação em vetores para cometer crimes (ALEXANDROU, 2019). Nos últimos anos, o padrão e a força dos ataques cibernéticos aumentaram rapidamente, conforme detectado pelo Fórum Econômico Mundial em seu estudo de 2018 (p. 33): "As capacidades de ataque cibernético estão crescendo mais rapidamente do que nossa capacidade de lidar com incidentes hostis".

Os ataques cibernéticos representam uma ameaça crescente não apenas à segurança pública, mas também à competitividade econômica de determinado país. As IC apresentam desafios de segurança cibernética peculiares devido à natureza específica da engenharia operacional e dos sistemas de energia comercial, que consistem em máquinas em rede, sensores, informações e softwares (PASQUALETTI *et al*, 2013). Para Pasqualetti *et al* (2013) as IC, em particular, são suscetíveis a ameaças, incluindo destruição de transações, modificação de informações e padrões de produtos e roubo de propriedade intelectual, pois os sistemas ciber-físicos são onipresentes em sistemas de energia, redes de transporte, processos de controle industrial, enfim, permeiam as áreas das infraestruturas críticas. Esses sistemas precisam operar de forma confiável diante de falhas imprevistas e ataques maliciosos externos.

Em âmbito nacional, o Exército Brasileiro (2017, define que ataque cibernético:

> É a atividade que tem o objetivo de interromper, negar o uso, degradar, corromper ou destruir sistemas computacionais ou informações armazenadas em dispositivos e redes computacionais e de comunicações de interesse. (EXÉRCITO BRASILEIRO, 2017, p. 27)

Interessante notar que existe algum consenso sobre a definição de ataque cibernético, e, como afirmam TU *et al* (2020), os ataques cibernéticos atuam sobre os pilares da Segurança da Informação: disponibilidade, confidencialidade e integridade.

2.3 INFRAESTRUTURAS CRÍTICAS

O conceito de infraestrutura crítica tem por objetivo descrever os sistemas e ativos físicos e cibernéticos que são tão vitais para o Estado que sua interrupção ou destruição teria um impacto debilitante em sua segurança física, econômica ou na segurança pública.

A infraestrutura crítica de uma nação fornece, desta forma, os serviços essenciais que sustentam a sua sociedade (KATTEL; AROS-VERA, 2020).

No contexto brasileiro, o artigo 2º da Portaria nº 2 do GSI/PR de fevereiro de 2008, definiu infraestrutura crítica como sendo "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional", dividindo-as em cinco áreas: energia, transporte, água, telecomunicações e finanças. Posteriormente, através da Portaria nº 53 do GSI de julho de 2018, foi acrescentada mais uma área: biossegurança e bioproteção.

3 METODOLOGIA

A metodologia utilizada nessa pesquisa foi a Revisão Sistemática da Literatura (RSL), baseada nas diretrizes propostas por Kitchenham e Charters (2007). As buscas foram realizadas nas bases de dados digitais *Web of Science*, *SCOPUS*, *IEEE Xplore* e *Google Scholar* e conduzidas pelo título, resumo e palavras-chave dos trabalhos encontrados, com exceção do *Google Scholar*, onde foram baseadas somente no título, entre os dias 20/09/2020 e 05/10/2020.

Quais foram as Áreas de Infraestruturas Críticas que mais sofreram ataques exitosos de Guerra Cibernética?, as buscas foram dirigidas a encontrar artigos que fossem capazes de respondê-la. Para a seleção dos estudos foi realizada a escolha das pesquisas nas bases de dados a partir dos critérios definidos no protocolo de revisão e relacionados à questão de pesquisa, que foram sumarizados no Quadro 1.

Para atender a esse artigo foram selecionados três constructos, a saber:

a) constructo 1, C1: Guerra Cibernética ou *Cyber Warfare*;
b) constructo 2, C2: Ataque Cibernético ou *Cyber Attack*;
c) constructo 3, C3: Infraestrutura Crítica ou *Critical Infrastructure*.

Quadro 1 – Critérios de busca

Número do critério	Descrição dos critérios de Inclusão
1	Os termos da pesquisa incluíram as palavras-chave Guerra Cibernética, Ataque Cibernético e Infraestrutura Crîtica no título ou no resumo (em português e inglês);
2	Foram incluídos artigos de revistas e artigos de congressos e conferências;
3	Foram excluídos artigos que não estivessem relacionados com Infraestruturas Crîticas ou com ataques cibernéticos exitosos;
Número do critério	**Descrição dos critérios de Exclusão**
4	Foram excluídos artigos que não fossem de acesso livre;
5	Foram excluídas monografias, dissertações e teses acadêmicas;
6	Foram excluídas pesquisas repetidas ou com estudos de caso repetidos.

Fonte: Autor, 2020.

Para a extração dos dados foi realizada a leitura dos artigos onde buscou-se relacionar a área de IC que foi atacada com êxito, o país ou região que sofreu o ataque, dando preferência a países, para evitar subjetividade, e o ano em que o ataque ocorreu.

Para a fase de sintetização dos dados extraídos foi elaborada uma tabela com o país/região afetada, a área de IC atingida, o ano e a referência do artigo.

Essa tabela, presente no Apêndice, permitiu a confecção dos gráficos que auxiliaram na análise do estudo e na resposta à questão de pesquisa.

4 RESULTADOS E DISCUSSÃO

A partir dos constructos citados foram realizadas cinco pesquisas distintas nas bases de dados digitais conforme apresentadas na Tabela 1.

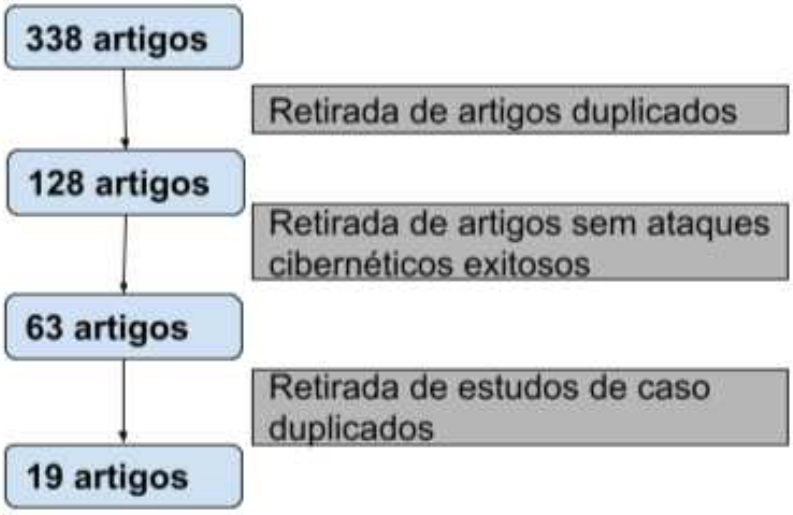
Tabela 1: Relação de Consultas X Resultados Obtidos por Bases

Consulta	Constructo	Resultados *Scopus*	Resultados *Web of Science*	Resultados *IEEE Xplore*	Resultados *Google Scholar*	Totais
Consulta 1	C1	794	373	243	1.370	2.780
Consulta 2	C2	8.748	1.631	1.402	2.090	13.871
Consulta 3	C3	10.214	4.197	2.013	5.940	22.364
Consulta 4	C1 e C3	57	25	13	4	99
Consulta 5	C2 e C3	28	105	78	29	239

Fonte: Autor, 2020.

A soma das consultas 4 e 5 resultou em 338 artigos. Em seguida os estudos foram selecionados com base no protocolo definido na metodologia, tendo como resultado a seleção de 19 artigos, conforme a Figura 1.

Figura 1— Seleção dos artigos



Fonte: Autor, 2020

Foi elaborado um quadro resumindo os 19 artigos encontrados e relacionando a área de Infraestrutura Crítica atingida, o país a que pertencia a área e o ano em que o ataque ocorreu. Esse quadro encontra-se no Apêndice.

Para identificar quais as áreas de IC que mais sofreram ataques cibernéticos esse artigo utilizou-se do diagrama de Pareto. O diagrama de Pareto é uma ferramenta que permite classificar em ordem decrescente de importância os critérios apresentados em formato de lista e que causam um efeito importante em um determinado assunto sendo pesquisado ou tratado (ARNOLD, 2014).

A Tabela 2 apresenta o cálculo da frequência de ocorrência dos ataques, da porcentagem deles e a porcentagem acumulada de cada fator nos estudos analisados, conforme exige o diagrama de Pareto.

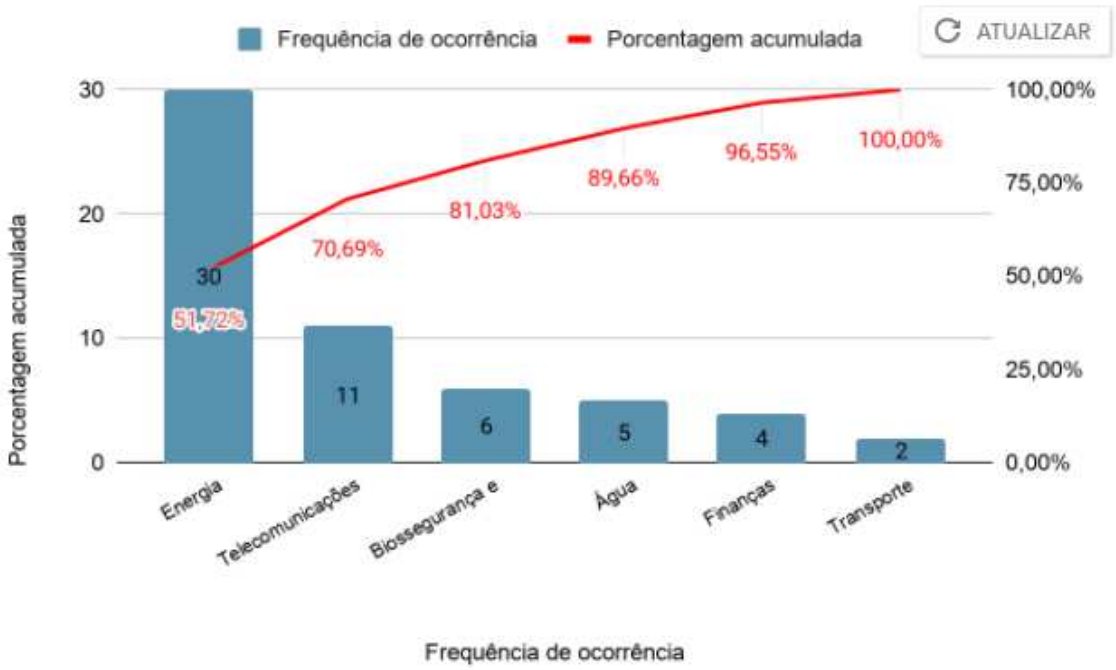
Tabela 2— Frequência de ocorrência de ataques às Infraestruturas Críticas

Área de Infraestrutura Crítica	Frequência de ocorrência	Porcentagem acumulada	Porcentagem
Energia	30	51,72%	51,72%
Telecomunicações	11	70,69%	18,97%
Biossegurança e Bioproteção	6	81,03%	10,34%
Água	5	89,66%	8,62%
Finanças	4	96,55%	6,90%
Transporte	2	100,00%	3,45%
Total:	58		

Fonte: Autor, 2020

Tendo-se os cálculos dos ataques às áreas de IC, apresentados na Tabela 2, aplicou-se o Diagrama de Pareto com os resultados apresentados no Gráfico 1, representando a frequência da ocorrência de cada fator e a porcentagem acumulada.

Gráfico 1—Diagrama de Pareto sobre as Áreas de Infraestruturas Críticas

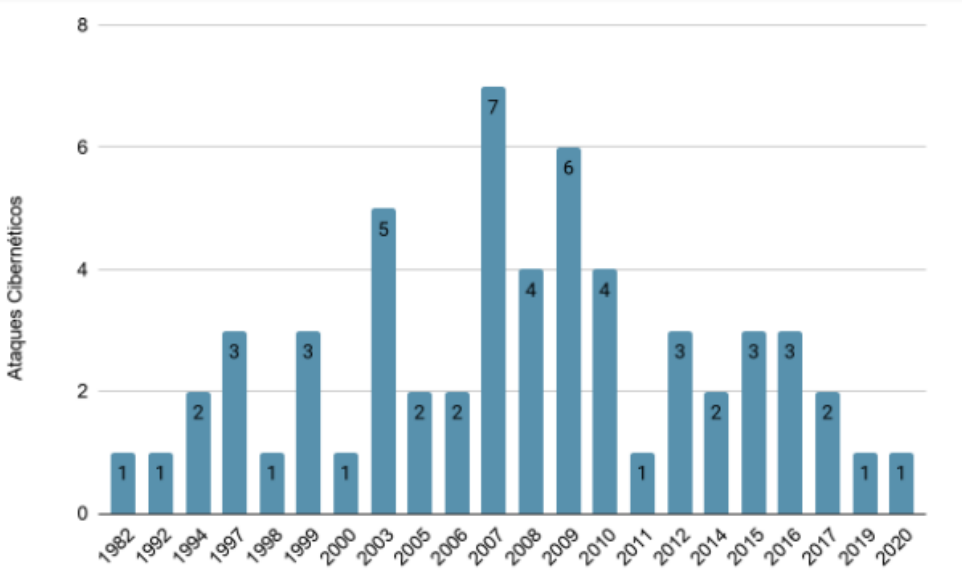


Fonte: Autor, 2020

Os resultados demonstrados pela aplicação do Diagrama de Pareto (Gráfico 1) indicam que as Áreas de Infraestruturas Críticas mais atingidas foram: Energia (51,72%), Telecomunicações (18,97%), Biossegurança e Bioproteção (10,34%). Essas três áreas de IC representam (81,03%) da frequência de ocorrência, significando que configuram as áreas de IC que mais sofreram ataques exitosos de Guerra Cibernética.

É interessante notar, no Gráfico 2, que nos anos de 2007 e 2009 houveram picos de ataques às ICs. Para Czossec *et al* (2011) os ataques, supostamente russos, destinados à Estônia em 2007 foram a primeira vez que o termo Guerra Cibernética tomou a manchete dos jornais, crescendo um interesse acadêmico.

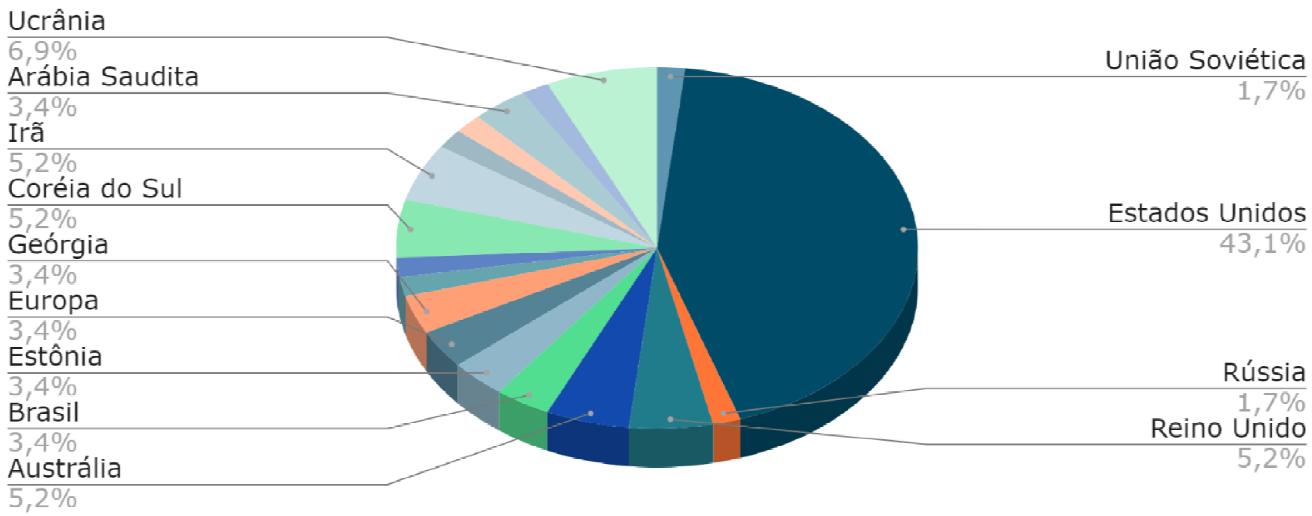
Gráfico 2—Quantidade de ataques por ano



Fonte: Autor, 2020

Como países e regiões mais afetadas pelos ataques, os Estados Unidos despontam em primeiro lugar, corroborando a afirmação de Duić *et al* (2017) de que a causa de sua vulnerabilidade é a sua dependência de computadores em rede e comunicação por computador. Outro país bastante afetado é a Ucrânia, em instabilidade territorial desde 2014, quando a Rússia anexou a região da Crimeia.

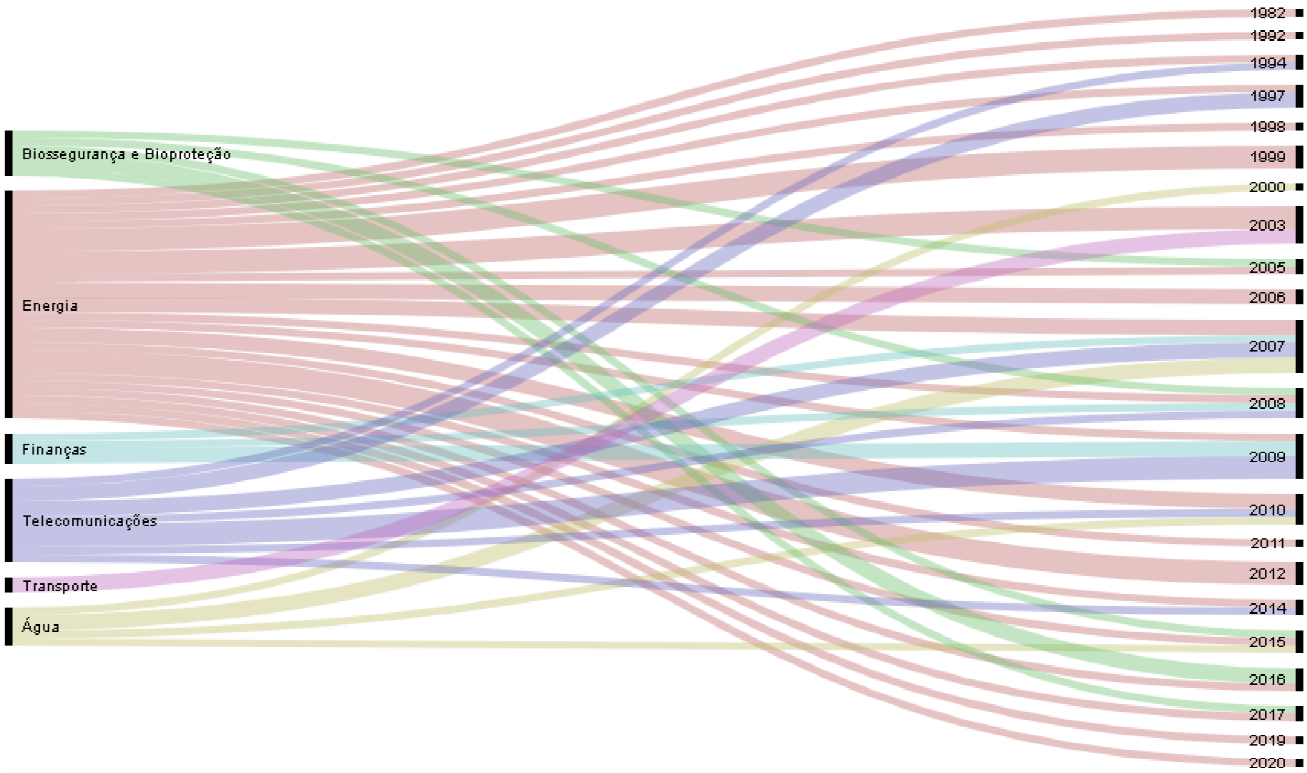
Gráfico 3 - Países e regiões mais afetadas pelos ataques



Fonte: Autor, 2020.

É possível observar, no Gráfico 4, a grande abrangência temporal da ocorrência de ataques na área de Energia.

Gráfico 4 - Relação entre as Áreas de ICs atingidas e os anos

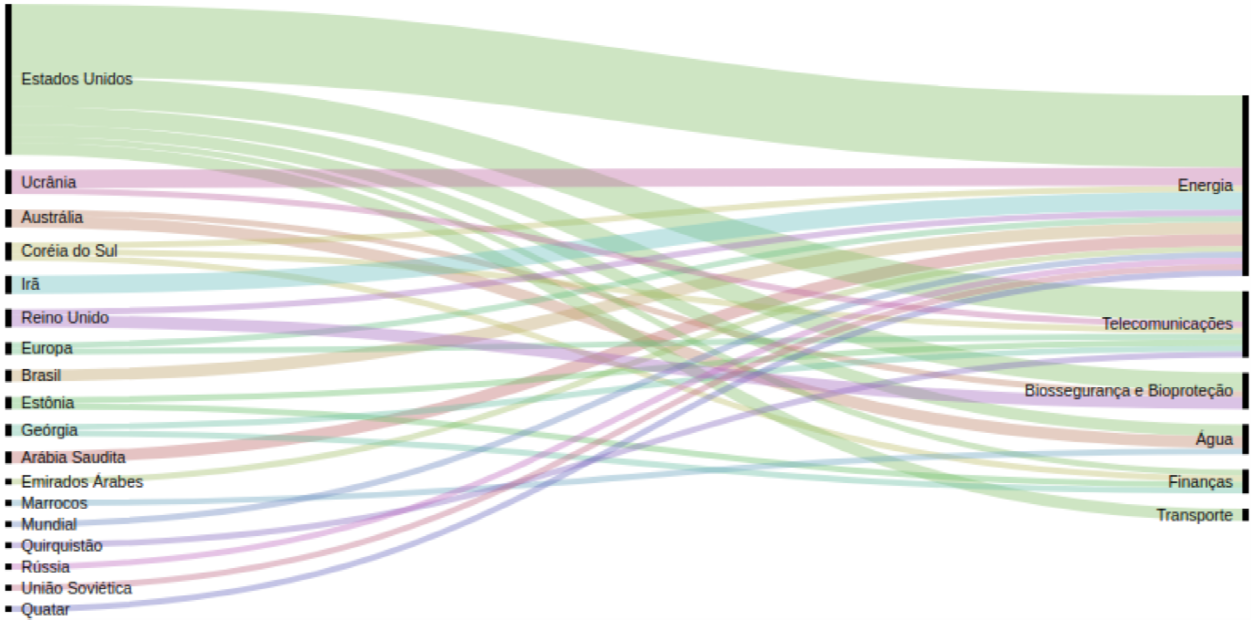


Fonte: Autor, 2020.

O Gráfico 5 demonstra que quase todos os países/regiões já sofreram ataques exitosos nas IC de Energia. Como afirmam Kovacevic e Nikolic (2015), no início do uso de sistemas SCADA, largamente utilizados para gerenciamento das IC da área de Energia, o objetivo era alcançar um bom desempenho e rede a segurança dificilmente era uma preocupação, já que a preocupação dominante era a segurança física e até recentemente estas redes foram isoladas para que um invasor não pudesse acessá-las.

Mas hoje há uma grande demanda por interconectividade entre sistemas SCADA e redes corporativas, o que se tornou uma brecha para ataques. Para Kalech (2019), outra vulnerabilidade é que os sistemas SCADA adotam, muitas vezes, a segurança por obscuridade, isto é, pelo fato de o sistema não estar disponível para o grande público, entende-se que atacantes terão dificuldades em testá-lo e invadi-lo, porém tem isso tem sido apontada como uma estratégia falha. Upadhyay e Sampalli (2020) acrescentam que muitas IC que utilizam sistemas SCADA têm políticas de segurança falhas, não mantendo os sistemas atualizados e nem recomendações das normas de segurança das informações exigidas como, por exemplo, ISO 27000.

Gráfico 5 - Relação entre países/regiões e áreas de ICs atingidas



Fonte: Autor, 2020.

5 CONCLUSÃO

O estudo foi conduzido através de uma pesquisa acadêmica na literatura disponível, realizada com os termos Guerra Cibernética, Ataque Cibernético e Infraestruturas Críticas. A pesquisa utilizou as bases de dados digitais *Web of Science*, *SCOPUS*, *IEEE Xplore* e *Google Scholar*. Foram aplicados critérios de inclusão e exclusão com a finalidade de encontrar as áreas de IC que mais sofreram ataques cibernéticos exitosos.

Os três constructos analisados nessa pesquisa, Guerra Cibernética, Ataque Cibernético e Infraestruturas Críticas se inter-relacionam, pois, a guerra tradicional extrapola as três dimensões existentes e tem sido aplicada com êxito na dimensão cibernética buscando impactar o mundo físico. Essa evolução tem trazido novas perspectivas para a defesa das Infraestruturas Críticas, que demandam, cada vez mais, proteções cibernéticas tanto para ataques diretamente direcionadas a elas, como ataques cibernéticos genéricos que podem impactá-las.

Os resultados obtidos na pesquisa indicam que a Área de Infraestrutura Crítica que mais sofreu ataques cibernéticos exitosos foi a de Energia. Foi possível observar a ocorrência desses ataques em uma grande miríade de países e regiões e em praticamente todos os anos em que houve relatos. Em resumo, isso significa que a Defesa Nacional, em particular no Exército, os integrantes do Sistema de Guerra Cibernética do Exército (SGCEx) devem estar particularmente atentos às possíveis vulnerabilidades que possam surgir nessa área de IC, pois embora não tenhamos sido alvos prioritários de Guerra Cibernética, novas modalidades de ataques podem atingir, indiretamente, o mundo todo.

Como limitação da pesquisa há de se salientar que foi realizada em um ambiente estritamente acadêmico, relatórios de ataques que não estivessem presentes em artigos ou publicações científicas foram descartados. Pesquisam futuras poderão incluir esses relatórios e, desta maneira, contribuir para uma análise mais apurada ou mesmo procurar avaliar o porquê dessas IC terem sido atacadas com êxito.

REFERÊNCIAS BILIOGRÁFICAS

AKPINAR, Kevser Ovaz; OZCELIK, Ibrahim. Analysis of machine learning methods in EtherCAT-based anomaly detection. **IEEE Access**, v. 7, p. 184365-184374, 2019.

AL-ABASSI, Abdulrahman et al. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. **IEEE Access**, v. 8, p. 83965-83973, 2020.

ALEXANDROU, Alex. Cybercrime. **International and Transnational Crime and Justice**, v. 10, p. 61, 2019.

ALFORD, Lionel D. **Cyber warfare**: a new doctrine and taxonomy. United States Air Force, 2001.

ARNOLD, Barry C. **Pareto distribution**. Wiley StatsRef: Statistics Reference Online, p. 1-10, 2014.

AZMI, Ida Madieha Abdul Ghani; ZULHUDA, Sonny; JAROT, Sigit Puspito Wigati. Data breach on the critical information infrastructures: lessons from the Wikileaks. **Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)**. IEEE, 2012. p. 306-311.

BAYLON, Caroline. Lessons from Stuxnet and the realm of cyber and nuclear security: implications for ethics in cyber warfare. **Ethics and Policies for Cyber Operations**. Springer, Cham, 2017. p. 213-229.

BLANK, Stephen. Cyber war and information war a la russe. **Understanding Cyber Conflict: Fourteen Analogies**, p. 1-18, 2017.

BODDY, Aaron *et al*. A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. **Proceedings of the 1st International Conference on Internet of Things and Machine Learning**. 2017. p. 1-7.

CARVALHO, Paulo Sérgio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos - Revista das Ciências Militares**, 2011.

CHEN, Thomas M. Stuxnet, the Real Start of Cyber Warfare? **IEEE Network**, v. 24, no. 6, 2010, p. 2–3.

COLEMAN, Kevin. The weaponry and strategies of digital conflict. **International Conference on Cyber Warfare and Security**. Academic Conferences International Limited, 2010. p. 491.

COLLINS, Aengus *et al*. The global risks report 2018. Genebra: **Fórum Econômico Mundial**. 2018.

CONOVALU, Sergiu; PARK, Joon S. Cybersecurity Strategies for Smart Grids. **Journal of Computers**, v. 11, n. 4, p. 300-309, 2016.

CZOSSECK, Christian; OTTIS, Rain; TALIHÄRM, Anna-Maria. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. **International Journal of Cyber Warfare and Terrorism (IJCWT)**, v. 1, n. 1, p. 24-34, 2011.

DUIĆ, Igor; CVRTILA, Vlatko; IVANJKO, Tomislav. International cyber security challenges. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). **IEEE**, 2017. p. 1309-1313.

EXÉRCITO BRASILEIRO. Comando de Operações Terrestres. **Manual de Campanha** EB-70-MC-10.232 Guerra Cibernética, Brasília: COTer, 2017.

HATHAWAY, Oona *et al*. The law of cyber-attack. **California Law Review**, p. 817-885, 2012.

JENIK, Aviram. Cyberwar in Estonia and the Middle East. **Network Security**, v. 2009, n. 4, p. 4 -6, 2009.

KATTEL, Prakash Jamar; AROS-VERA, Felipe. Critical infrastructure location under supporting station dependencies considerations. **Socio-Economic Planning Sciences**, v. 70, p. 100726, 2020.

KALECH, Meir. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. **Computers & Security**, v. 84, p. 225-238, 2019.

KOETSEV, Viktor. Saudi Arabia in the firing line. **Petroleum Economist**. 2019. Disponível em: https://www.petroleum-economist.com/articles/politics-economics/middle-east/2019/saudi-arabia-in-the-firing-line. Acesso em: 05 Out. 20.

KITCHENHAM, Barbara; CHARTERS, Stuart. **Guidelines for performing systematic literature reviews in software engineering**. EBSE Technical Report EBSE-2007-01, Keele University e University of Durham. 2007.

KOVACEVIC, Ana; NIKOLIC, Dragana. Cyber attacks on critical infrastructure: Review and challenges. **Handbook of Research on Digital Crime**, Cyberspace Security, and Information Assurance. IGI Global, 2015. p. 1-18.

LEE, Kyung-bok; LIM, Jong-in. The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd. KSII **Transactions on Internet & Information Systems**, v. 10, n. 2, 2016.

LIBICKI, Martin C. What is information warfare?. **National Defense Univ Washington DC Inst for National Strategic Studies.** 1995.

LO, Huai-Wei et al. A new soft computing approach for analyzing the influential relationships of critical infrastructures. **International Journal of Critical**

Infrastructure Protection, v. 28, p. 100336, 2020.

MANDARINO JUNIOR., R. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

MARTIN, Guy et al. Cybersecurity and healthcare: how safe are we?. **TheBMJ**, v. 358, 2017.

MINISTÉRIO DA DEFESA. Forças Armadas. **Glossário das Forças Armadas** - MD35-G-01, 5 ed., 2015.

MOȘOIU, Ovidiu. BĂLĂCEANU, Ion. MIHAI, Eduard. Cyber Terrorism and the Effects of the russian attacks on democratic States in East Europe. **Scientific Journal of Silesian University of Technology**, v. 106, 2020.

NICHOLSON, Andrew et al. SCADA security in the light of Cyber-Warfare. **Computers & Security**, v. 31, n. 4, p. 418-436, 2012.

ONYEJI, Ijeoma; BAZILIAN, Morgan; BRONK, Chris. Cyber security and critical energy infrastructure. **The Electricity Journal**, v. 27, n. 2, p. 52-60, 2014.

PARKS, Raymond C.; DUGGAN, David P. Principles of cyberwarfare. **IEEE Security & Privacy**, v. 9, n. 5, p. 30-35, 2011.

PASQUALETTI, Fabio, et al. Attack Detection and Identification in Cyber-Physical Systems. **IEEE Transactions on Automatic Control**, v. 58, n. 11, p. 2715–2729, 2013.

PROCTOR, Matt; SMITH, Terry. Lessons learned from NERC CIP applied to the industrial world. **2017 70th Annual Conference for Protective Relay Engineers (CPRE)**. IEEE, 2017. p. 1-6.

ROBINSON, Michael; JONES, Kevin; JANICKE, Helge. **Cyber warfare**: issues and challenges. Computers & security, v. 49, p. 70-94, 2015.

SHAHEEN, Salma. Offense–defense balance in cyber warfare. **Cyberspace and International Relations**. Springer, Berlin, Heidelberg, 2014. p. 77-93.

SHIRAZI, Syed Noorulhassan et al. Evaluation of anomaly detection techniques for scada communication resilience. **2016 Resilience Week (RWS)**. IEEE, 2016. p. 140-145.

STEVENS, Clare. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. **Contemporary Security Policy**, v. 41, n. 1, p. 129-152, 2020.

SUGUMAR, Gayathri; MATHUR, Aditya. Testing the effectiveness of attack detection mechanisms in industrial control systems. **2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)**. IEEE, 2017. p. 138-145.

THAKUR, Kutub et al. Impact of cyber-attacks on critical infrastructure. **2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity**. IEEE, 2016. p. 183-186.

UPADHYAY, Darshana; SAMPALLI, Srinivas. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. **Computers & Security**, v. 89, p. 101666, 2020.

TU, Haicheng et al. A Hybrid Cyber Attack Model for Cyber-Physical Power Systems. **IEEE Access**, v. 8, p. 114876-114883, 2020.

WEINBERGER, Sharon. **How Israel Spoofed Syria's Air Defense System**.Wired, 4 de Outubro, 2007. Disponível em: https:// www.wired.com/2007/10/how-israel-spoo/. Acesso em: 05 set. 2020.

*Artigo realizado a partir do trabalho de conclusão do Curso de Especialização em Guerra Cibernética do Centro de Instrução de Guerra Eletrônica em 2020 pelo 1º Ten Barbosa Oliveira, instrutor do Curso de Comunicações do Centro de Preparação de Oficiais da Reserva de São Paulo – CPOR/SP. Endereço postal: Rua Alfredo Pujol, 681 - Santana - São Paulo/SP - CEP: 02017-011. E-mail: barbosaoliveira.joao@eb.mil.br.