

Tilburg University

The impact of cyberattacks on small states

de Nobrega, Kristel; Rutkowski, Anne F ; Ribbers, Piet

Published in:
IEEE Software

DOI:
[10.1109/MS.2023.3265130](https://doi.org/10.1109/MS.2023.3265130)

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
de Nobrega, K., Rutkowski, A. F., & Ribbers, P. (2023). The impact of cyberattacks on small states. *IEEE Software*, 40(4), 101-105. <https://doi.org/10.1109/MS.2023.3265130>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



The Impact of Cyberattacks on Small States

Kristel M. de Nobrega, Centrale Bank of Aruba
Anne-Francoise Rutkowski^{ID} and Piet Ribbers, Tilburg University

From the Editor

The “Impact” series has often emphasized the importance of size and volume to survive in software and IT. But what if the size of your country is small and you face the same cyberthreats as much larger countries in the world? That is the case with small states that face the same cyberattacks while often having less means to defend themselves. You cannot grow a small state into a large state just to be able to defend yourself better against cyberattacks. What you can do is explained in this column.

—Les Hatton and Michiel van Genuchten

AT THE TIME of writing this column, Russia and Ukraine are at war. Cyberattacks are part of the weapon arsenal in use. Cyberattacks have been launched on the central Bank of Poland targeting distributed denial of service (DdoS). In parallel, Israel reports its largest DdoS to date hitting government websites, making them unavailable. Also, the hacktivist group Anonymous is threatening to release proof related to a breach of the Russian Central Bank. The danger of escalating global conflicts in cyberspace is a hard reality. The

National Atlantic Treaty Organization (NATO) has pronounced that a serious cyberattack on any of its members would trigger collective defense under Article 5. In a time of escalating tension with Russia and China, small states are in a difficult situation. Small states, such as the Pacific small island states, European landlocked countries, Baltic states, and the Caribbean region small open economies represent about a quarter of World Bank members. Those in the Asia–Pacific basin lack cyber forensic capability to gather enough evidence to substantiate geopolitically sensitive attribution. Mostly, even when attribution could be

made, small states will choose peace over war, as market trade is essential to their survival and offense is not on their agenda. Small states in the Caribbean region are a perfect “sandbox” that enables attackers to test in an isolated setting the orchestration of their malicious activities.

In November 2019, a ransomware attack was launched on the only hospital in Aruba. The digital patient information systems became inaccessible, forcing the staff to fall back on to a manual system to ensure patients’ care. In St. Martin, a black byte ransomware attack was launched on the national electrical grid locking out computers. The attackers paralyzed

Digital Object Identifier 10.1109/MS.2023.3265130
Date of current version: 14 July 2023

billing to customers and generated disconnections due to defaulters. In the financial sector, the Pan American Life Insurance Group operating from the United States and in the Caribbean got hit by a REvil ransomware attack.¹ Claims found on the dark web amount to 170 GB of stolen files as a result of the breach. In 2021, Microsoft’s Digital Crimes Unit seized the websites of think tanks and human rights organizations of 29 countries (including Barbados, Dominican Republic, Jamaica, Trinidad, and Tobago).² Microsoft concluded that these websites would serve as launching base for intelligence-gathering purposes by the China-based hacking group *Nickel*.

The current costs of initiating cyberattacks seem to be lower than the cost of incident response and remediation. For example, costs to conduct an advance persistent threat (APT) sophisticated attack have been estimated between US\$65,000 and US\$542,000.³ The cost to clean up is reported for 2022 to be US\$4.35 million. One of the most dangerous traits of APT is the ability to run the background process silently, for example placing secured unnoticed back doors. The path to attack takes longer, as the aim of the adversary is to have long persistence. The high level of disguise and

sophistication of APT make it difficult for organizations to notice. Hence, costs will only increase through time. APTs have been attributed to nation states with aggressive cyber defensive and offensive capabilities.

Small states experience more limitations in building capacity and developing cyber capability compared to nation states. Cybersecurity capacity is linked to variables, such as gross domestic product (GDP), that form a proxy for the available resources or cybersecurity capacity. Indeed, economies of scale and the availability of more financial and personnel resources allow deploying more controls, and therefore enhance the organizational capability in protecting the organization, hence the level of security maturity. Aruba has requested help from the Estonian e-Governance Academy (EGA 2022). Estonia became a leader in cyberdefense when it bounced back from its infamous cyberattack in 2007. It became a driving force in the European Union, proposing an integral national cyber strategy in 2008.⁴ Estonia has a small GDP of approximately €187 billion and spends the NATO recommendation of at least 2% of their GDP on defense. This is nearly the entire GDP of a small state, such as Aruba.

Insight Into Small States Perception of Cyber Defense and Offense

Thirteen information security leaders from the Cybersecurity Information Sharing Group (CISG) banded to the Caribbean region reported in a survey the frequency of cyber classes of attacks observed in the last 6 months (Table 1).

Also, we interviewed six chief information security officers (CISO) operating on the main critical infrastructures of Aruba. They mostly converge with the idea that a cyber defender in Aruba should know more about the “whole cyber picture” than a cyber expert in a larger state “who would have the luxury to know ‘only’ a small part in a particular area.” The cyber competition is an offense-dominant clash. Particularly, when attackers and defenders are given equal resources, the attacker will usually prevail.⁵ Attackers favor the offense because it offers anonymity, preventing meaningful deterrence.⁶ For small state and for small enterprise, an offensive posture seems particularly challenging, not to say a “nonoption.” One CISO commented on the stark lack of resources on the island in term of resources or cyber talent during the interview. Lack of technological and human resources is a major argument to rely further on security software and hardware on the island (e.g., sandbox, network monitoring, honeypot). Such technologies facilitate a data-driven approach in detecting more cyber threats, reducing de facto human intervention and bias.

Can Artificial Intelligence Be of Help to Cyber Experts?

It makes sense to investigate how artificial intelligence (AI) can contribute processing the data generated in cyberdefense. In 2023, it seems that

Table 1. Observed cyber offense in the last 6 months from least (1) to most (5) frequently observed (CISG).

Attack class	Median	Mode	% Most frequent score
Probing attack	5	5	53.8%
Denial of service	2	2	7.7%
Remote to local (user) attacks	2	2	7.7%
User to root attacks	1	1	7.7%
Payload attacks	3	1–4	23.1%

AI is supposed to aid in finding the solution to all problems in the world. This research started years back and reality is more stubborn. One CISO indicated that technical controls “are not a one-stop solution for cybersecurity.” The interviewee emphasized that the speed of which vulnerabilities are being exploited by attackers is accelerating. Hence, specific proactive actions are required in, for example, deploying extra technologies to defend the organization. As another participant stated, “cybercriminals

are becoming so advanced that you have to check more than in the past, when it was just checking the virus in the virus database. Right now, they are using all other strategies that the behavior needs to check, and certain triggers need to go through ... more of what is going on.” Another participant confirmed that, “a proactive approach should happen before the project goes live. Hence the human will be the last one holding the key and taking decision regarding security.”

Thirty-eight members of the Operational Security Situational Awareness Teleconference (OSSAT) rated statements regarding the future of AI. [OSSAT has been organized by the European Central Bank since 2012 for sharing information on cybercrime in the financial services sector, vulnerabilities, technological trends and threats, and security incidents. The membership is limited to members of the Bank for International Settlements, international financial institutions (International Monetary

Table 2. The future of AI according to OSSAT members, rated on a scale from strongly disagree (1) to strongly agree (7).

#	Quotations	Mean	Standard deviation	Mode
1	Model learning and resourcing takes time with current AI technology.	5.29	1.20	6
2	AI systems' learning may be the next target.	5.24	1.40	6
4	The human ability to improvise will remain important.	4.58	0.64	5
5	A broad hybrid combination of humans alongside AI agents and ethics are important to combat the hackers.	4.45	0.72	5
6	AI agents will be supportive to my work, not take over it.	4.34	0.71	4
7	AI agents will make us adapt to new ways of working.	4.32	0.62	4
8	Human input will remain key the coming years.	4.16	0.68	4
9	More people will be working with algorithms in the next coming years.	4.08	0.75	4
10	The human ability to make quick shots will remain key.	4.08	1.1	5
11	AI agents will evolve into a strategic technology for security specialists.	4.08	0.85	4
12	AI agents will not replace ethics.	4.05	1.06	4
13	Within 10 years there will be more autonomous AI agents taking over human tasks.	3.97	0.79	4
14	In the future it will be AI agents attacking against AI agents defending the organization.	3.66	0.94	4
15	AI agents will require a new edge of reasoning we may not be prepared for yet.	3.29	0.77	3
16	In the coming years some countries may be putting AI agents in jail.	1.92	0.88	2

ABOUT THE AUTHORS



KRISTEL M. DE NOBREGA is a manager of information security at the Centrale Bank of Aruba, Oranjestad, Aruba. Contact her at k.denobrega@cbaruba.org.



ANNE-FRANÇOISE RUTKOWSKI is a full professor in management of information at the Tilburg School of Economics and Management, Tilburg University, 5037 Tilburg, The Netherlands. Contact her at a.rutkowski@tilburguniversity.edu.



PIET RIBBERS is an Emeritus professor of information management, dean of the School of Economics, and head of Department of Information Systems and Management at Tilburg University, 5037 Tilburg, The Netherlands Contact him at p.m.a.ribbers@tilburguniversity.edu.

In March 2023 (when we finished writing this column), *Wired* announced that “Microsoft’s ‘Security Copilot’ Unleashes ChatGPT on Breaches.”⁹

What may the future bring? The Data Breach Investigation Report in 2022 shows that 82% of breaches involved a human element.¹⁰ Education, collaboration, and organization are key in the fight against cyberattacks, also for small-states. Interestingly, the majority of the stakeholders mentioned unity of effort to be important to defend properly. One CISO emphasized the importance of having this principle sorted out prior to an island-wide cyberattack, as “there should be an entity or body that would take the decision at that moment to decide who goes first in order of assistance if all are hit together.” Security experts on the island believe that AI will aid cyberdefense professionals. Madnick stated, “The good guys are getting better, but the bad guys are getting badder faster.”¹¹ As we indicated before in the series of “Impact” columns: “The benefits that legitimate developers enjoy are exactly the same for people who want to use software for criminal purposes.”¹² The rat race is still on, with another tool in the arsenal of the good and the bad guys. One more example: When asking ChatGPT to generate some malware, it will first provide a politically correct answer. However, in February 2023, it was already reported that cybercriminals bypass ChatGPT restrictions using the openAI API.¹³ The business model is already available, with some free queries, after which the price is an amount of money per 100 queries. The bad guys already figured out the integration of ChatGPT in their business model, while many legitimate companies have just started


Fund, World Bank), members of the European System of Central Banks, and the Computer Emergency Response Team for the European Union institutions, bodies, and agencies.] These 16 statements were originally collected via a focus group interview of cyber experts in the financial sector on the island Aruba.⁷ Results are presented in Table 2, from highest to lowest score of agreement.

The top quote in Table 2 (#1) relates directly to the struggle small states face when lacking resources and time to defend. Information security specialists perceive the role of AI agents versus human rather positively (quotes #4, #6, #7, #8, #9, #10, #13). Still, there is little hope that AI and data fusion will leave a great space in terms of improvisation in cyberspace to human. Participants agree that a broad hybrid combination of humans

alongside AI agents and ethics is important to combat hackers, and that humans will not be substituted by AI ethics (quote #5). For example, AI systems could be a support for forensic analysis that is required but lacking in small states, such as Aruba. AI can help in predicting the occurrences or reoccurrences of actual or potential criminal offences based on profiling of natural persons, based on a collection of past criminal behavior. The idea that in the future AI agents would end up in jail (quote #16) belongs probably to science fiction. A European Union proposal aims at extending a specific legal status to machines, holding these systems legally responsible for their actions.⁸

Outsourcing cyberdefense to Big Tech will, for more nations, entail a new form of legal sociopolitical challenge. AI holds a lot of promise for small states.

thinking about how to use ChatGPT in the first place.

The inherent limitations of small states, such as the Caribbean islands, with their focus on neutrality, metaphorically resembles fighting with wooden sticks against giants' elaborate attacks. What can we learn from the military, who have been in the defense business for a much longer time and consider cybersecurity very serious these days? The notion of *fighting power* has been applied to cyber defense.¹⁴ Fighting power consists of three components: the *physical component* that relates to the "means to operate and fight," the *moral component* that relates to "people's will and ability to get people to operate and fight," and the *conceptual component* that addresses the "ideas behind how to operate."¹⁴ The physical component comprises hardware and software, both virtual and physical assets, as well as information. So AI will help, but is only part of one of the three fighting power components. As Newton demonstrated, "a body in motion tends to stay in motion unless acted on by an outside force." Combining moral, conceptual, and physical components is crucial to reach a complex synergy to defend a system's moment of inertia. Small states should gain stability rather than being pushed around by external forces, such as attackers, expensive technological innovation, and abundance of legislation hard to cope with. Greater collaboration would serve as a major force, ensuring a greater stability of a small-island defensive system, hence, putting a strong break on the cyber rat race. 

References

1. "T&T among several countries hit by cyberattacks from international

hacking group – Microsoft," *Guardian*, Dec. 2012. [Online]. Available: <https://www.guardian.co.tt/news/tt-among-several-countries-hit-by-cyberattacks-from-international-hacking-group--microsoft-6.2.1428159.21dafb6579>

2. "Microsoft seizes sites used by APT15 Chinese state hackers," *Bleeping Comput.*, Dec. 2021. [Online]. Available: <https://www.bleepingcomputer.com/news/microsoft/microsoft-seizes-sites-used-by-apt15-chinese-state-hackers/>

3. *Hack at All Cost: Putting a Price on APT Attacks*. (2019). Positive Technologies Security. [Online]. Available: <https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/>

4. N. Shafqat and A. Masood, "Comparative analysis of various national cyber security strategies," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 1, p. 129, Feb. 2016.

5. A. F. Krepinevich, "Cyber warfare a 'Nuclear Option?' Cyber warfare," Center for Strategic and Budgetary Assessments, Washington, DC, USA, 2012. [Online]. Available: https://www.files.ethz.ch/isn/154628/CSBA_Cyber_Warfare_For_Web_1.pdf

6. R. Slayton, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," *Int. Secur.*, vol. 41, no. 3, pp. 72–109, Jan. 2017, doi: 10.1162/ISEC_a_00267.

7. K. M. de Nobrega and A. F. Rutkowski, "The AI family: The information security managers best frenemy?" in *Proc. 55th Hawaii Int. Conf. Syst. Sci.*, 2022, pp. 184–193, doi: 10.24251/HICSS.2022.022.

8. "Laying down harmonized rules on artificial intelligence," European Commission, Brussels, Belgium, Apr.

2021. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>

9. "Microsoft's 'Security Copilot' unleashes chatGPT on breaches," *Wired*, Mar. 2023. [Online]. Available: <https://www.wired.com/story/microsoft-security-copilot-chatgpt-ai-breaches/>

10. "Data breach investigations report." Verizon. Accessed: Feb. 19, 2022. [Online]. Available: <https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2022-data-breach-investigations-report.pdf>

11. S. Madnick, "Preparing for the cyberattack that will knock out U.S. power grids," *Harvard Bus. Rev.*, pp. 1–6, May 2017. [Online]. Available: <https://cams.mit.edu/wp-content/uploads/2017-07.pdf>

12. A. F. Rutkowski, M. van Genuchten, and L. Hatton, "No free lunch for software after all," *IEEE Softw.*, vol. 34, no. 5, pp. 13–15, Sep. 2017, doi: 10.1109/MS.2017.3571570.

13. "How-hackers-can-abuse-ChatGPT-to-create-malware," *Techtarger*, Feb. 2023. [Online]. Available: <https://www.ghacks.net/2023/02/04/chatgpt-is-used-by-cybercriminals-to-write-better-phishing-emails/>

14. P. A. Ducheine, J. van Haaster, and R. van Harskamp, "Manoeuvring and generating effects in the information environment," in *Netherlands Annual Review of Military Studies 2017: Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, P. A. L. Ducheine and F. P. B. Osinga, Eds. The Hague, The Netherlands: T.M.C. Asser Press, 2017, pp. 155–179.