Why Great Powers Launch Destructive Cyber Operations and What to Do About It

Weber, Valentin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

No. 33
November 2023

DGAP POLICY BRIEF

Why Great Powers Launch Destructive Cyber Operations and What to Do About It

Valentin Weber
Senior Research Fellow,
Center for Geopolitics,
Geoeconomics,
and Technology

2010 was a seminal year. Stuxnet, an American-Israeli cyber operation sabotaged Iranian uranium enrichment centrifuges. It became publicly known as the first cyber operation in history that destroyed physical objects. This operation had the clear goal of degrading Iran's uranium enrichment capability, but in general there has been little research as to why hegemons launch destructive cyber operations. This brief argues that the main motivations are threefold: territorial conquest, threat prevention, and retaliatory actions.

- Iran, North Korea, South Korea, Ukraine and Taiwan have been the main targets of destructive great power cyber operations.
- For the US, future targets will possibly be limited to countries that aim to acquire nuclear weapons – Iran and North Korea
- Given ongoing border disputes, China and Russia will likely target neighboring countries with such destructive campaigns – for China those are Vietnam, the Philippines, and Japan, and for Russia they are Georgia, Moldova, and Japan.
- To prevent destructive cyber operations, Germany and other EU states have been engaged in cyber capacity building and threat-intelligence sharing across continents. But Berlin needs to set priorities.
- When it comes to combatting state-sponsored cyber campaigns, Germany should deepen ties with non-EU countries that have been or likely will be targets of damaging rather than merely disruptive operations, i.e., in Southeast Asia, East Asia, the Caucasus, and Southeast Europe.

When pundits and policy makers characterize the operations of great powers in cyberspace, they often label the United States as precise, responsible, and stealthy, China as loud, and Russia as reckless. This commonly held distinction between these actors has become less applicable as the great powers have increased such activities. In some recent operations, China has been very stealthy.[1] It has tried to remain covert and maintain long-term access to the systems it has breached . Russia, too, was surgical in its operation targeting Texas-based SolarWinds, one of the most sophisticated cyber operations in US history, which spread undetected for months to the company's clients, allowing Russian hackers to infiltrate major US corporations and government agencies.[2]

But this policy brief is not about how great powers conduct cyber operations. Rather, it examines an aspect that has been less explored. It aims to provide a comparative analysis of why hegemons conduct destructive cyber campaigns and to provide recommendations as to what Germany and other European Union member states can do to mitigate them.

This brief defines destructive cyber operations as having the following effects:

- Death or human injury
- Considerable physical damage
- Demolition or modification of information, making data useless if significant efforts are invested to make systems work again[3]

But there are a few caveats. It does not examine state behavior aimed at non-state actors (e.g., the US targeting ransomware gangs or Islamist extremist groups), nor does it explore cyber operations solely consisting of distributed denial of service (DDoS) attacks, which overwhelm servers with internet traffic, or website defacements (e.g., Russian attacks on Estonia and Georgia, both in the late 2000s), as those are mostly disruptive but not destructive.[4] This brief also does not examine cyber operations during large-scale hostilities where countries face each other in a major war (Russia attacking Ukraine in 2022). Here it is important to note that destructive cyberattacks, especially wipers (malware that destroys data), have been used frequently by Russia against Ukraine since its full-scale invasion in 2022.[5]

A SHORT HISTORY OF DESTRUCTIVE CYBER CAMPAIGNS

The sample size of destructive great power cyber operations targeting states outside of a major conflict is rather limited. Historically, there have been five series of destructive operations (i.e., cyber campaigns), which will be discussed in more detail below. These include the US targeting Iran's nuclear sector and databases (2010-2019) and North Korea's missile program (2014-2017), China targeting Taiwan's oil and gas, telecommunications, and other critical sectors (2020), and Russia inserting malicious code into a host of Ukrainian critical infrastructure (2015-2022) and systems of the Olympic games organizers in South Korea (2018). Each of these campaigns consisted of multiple cyber operations. In this brief, they count as one series of destructive cyber behaviors – a destructive cyber campaign.

US-Iran (2010-2019)

The first cyber campaign examined relates to the US-Iranian dyad. In 2010, a destructive cyber operation known as Stuxnet hit nuclear enrichment facilities in Natanz, Iran.[6] In addition, in 2019, the US disabled Iranian databases that Tehran had used to attack oil tankers in the Gulf.[7]

US-North Korea (2014–2017)

Since the mid-2010s, most North Korean missiles have exploded mysteriously, long before reaching their target. The US was alleged to have interfered with Pyongyang's missile program to delay and

1 Risky.Biz, "Between Two Nerds: China's Changing Cyber Espionage Playbook - Risky Business," August 8, 2023, https://risky.biz/BTN45.

2 Craig Timberg and Ellen Nakashima, "Russian Hack Was 'Classic Espionage' with Stealthy, Targeted Tactics," Washington Post, December 14, 2020, https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government.

3 Centre for Cybersecurity, "The Threat of Destructive Cyber Attacks," June 2021, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-threat-of-destructive-cyber-attacks.pdf.

4 Cyber operations, where DDoS attacks are part of the operation but not sole vector are included in this analysis, see for example 2016 attack on Ukrainian power grid. Amy Krigman, "Cyber Autopsy Series: Ukrainian Power Grid Attack Makes History," GlobalSign, September 27, 2022, https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history.

5 Andy Greenberg, "Ukraine Suffered More Data-Wiping Malware in 2022 Than Anywhere, Ever," Wired, February 22, 2023, https://www.wired.com/story/ukraine-russia-wiper-malware.

6 Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" (Langner Group, November 2013), https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

7 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," The New York Times, August 28, 2019, sec. U.S., https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

degrade its missile strike capabilities.[8] This may have been achieved by subverting supply chains and tampering with nuclear command and control systems.[9] According to a Reuters report, the US may have simultaneously targeted North Korean and Iranian nuclear programs.[10] While the US had been successful in Iran already in 2010, the cyber campaign in North Korea took a few years to show effects, and was helped by its reinforcement in early 2014 under then-President Barack Obama.[11]

Russia-Ukraine (2015-2022)

Even before Russia's full-scale invasion of Ukraine in 2022, the target of its most destructive operations appears to have been Ukraine. In 2015 and 2016, the GRU (Russia's military intelligence service) conducted operations against Ukraine's power grid.[12] In 2015, this resulted in six hours of power outages, affecting 225,000 customers.[13] In 2016, another Russian cyber operation knocked out a Kyiv electricity substation for around an hour.[14] Further destructive campaigns on state institutions affecting the Ministry of Finance and the State Treasury Service took place in 2016.[15] During the next year, the malware NotPetya, attributed to the GRU, hit Ukraine and the wider world causing significant destruction and economic costs.[16]

Russia-South Korea (2018)

In 2018, Russia targeted South Korea. Prior to the Pyeongchang Olympics in 2018, a cyber operation disabled the organizer's ticketing system, Wi-Fi and TV screens around several Olympic facilities.[17] A solid effort by the organizer's security defenders averted the worst. But even if major havoc was avoided, the cyber activity was destructive in nature, since it contained data-wiping components and obstructed data recovery procedures.[18] As Warren Mercer, threat researcher for Cisco Talos notes, "Wiping all available methods of recovery shows this attacker had no intention of leaving the machine useable. The purpose of this malware is to perform destruction of the host, leave the computer system offline, and wipe remote data."[19]

China-Taiwan (2020)

In May 2020, a wiper attack hit several critical infrastructure companies in Taiwan, including oil and gas importer Taiwan Chinese Petroleum (CPC), encrypting systems. In financially motivated attacks, a decryption key would have been offered in exchange for a ransom. The lack of a ransom component in this case makes a destructive intent plausible: "A closer look into the malware revealed this particular variant of ColdLock [malware] had removed all the payment information, contact email, and the RSA public key. This indicates that no information could be provided for decryption."[20] While the effect on the Taiwanese economy was to some extent disruptive (people couldn't use CPC payment cards to buy gas), affected data on CPC systems was deleted and rendered unusable due to encryption. CPC had to reconstruct some of its infrastructure after the cyber operation.[21] Taiwan's Ministry of Justice attributed the activities to

8 David E. Sanger and William J. Broad, "Hand of U.S. Leaves North Korea's Missile Program Shaken – The New York Times," *New York Times*, April 18, 2017, https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html.

9 Ankit Panda, "North Korea, US 'Left of Launch' Cyber Capabilities, and Deterrence," December 6, 2018, https://thediplomat.com/2018/12/north-korea-us-left-of-launch-cyber-capabilities-and-deterrence."language":"en-US","title":"North Korea, US 'Left of Launch' Cyber Capabilities, and Deterrence","URL":" https://thediplomat.com/2018/12/north-korea-us-left-of-launch-cyber-capabilities-and-deterrence"

10 Joseph Menn, "Exclusive: U.S. Tried Stuxnet-Style Campaign against North Korea but Failed - Sources," Reuters, May 29, 2015, sec. APAC, https://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.

11 David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times*, March 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

12 U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace | United States Department of Justice," October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

13 David E. Whitehead et al., "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," in 2017 70th Annual Conference for Protective Relay Engineers (CPRE), 2017, 1–8, https://doi.org/10.1109/CPRE.2017.8090056.

14 Joe Tidy, "Ukrainian Power Grid 'Lucky' to Withstand Russian Cyber-Attack," *BBC News*, April 12, 2022, sec. Technology, https://www.bbc.com/news/technology-61085480.

15 U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace | United States Department of Justice."

16 U.S. Department of Justice.

17 Andy Greenberg, "Inside Olympic Destroyer, the Most Deceptive Hack in History," WIRED, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack.

18 Warren Mercer, "Olympic Destroyer Takes Aim At Winter Olympics," Cisco Talos Blog, February 12, 2018, https://blog.talosintelligence.com/olympic-destroyer.

19 Mercer.

20 CyCraft Technology Corp, "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware," *CyCraft* (blog), June 10, 2022, https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5.

21 Sean Lyngaas, "Taiwan Suggests China's Winnti Group Is behind Ransomware Attack on State Oil Company," *CyberScoop* (blog), May 18, 2020, https://cyberscoop.com/cpc-ransomware-winnti-taiwan-china.

the Winnti Group, a threat cluster affiliated with the Chinese Ministry of State Security.[22]

More operations could have been included in this analysis, but were excluded due to non-definitive attribution claims. Those would have been China causing power outages in India in 2021 and shutting down a port in Japan in 2023, as well as the US causing explosions of a Russian gas pipeline in 1982.[23]

COMMONALITIES OF PAST DESTRUCTIVE CYBER CAMPAIGNS

Motivation – The Strong Do What They Can

All five cyber campaigns by the US, China, and Russia examined in this policy brief were conducted on national security grounds.

Beijing and Moscow have for some time been advancing territorial claims in Taiwan and Ukraine, respectively. The primary reason for the Russian cyber campaigns conducted between 2015 and 2022 was that Russia did not recognize Ukraine's territorial sovereignty and saw cyber operations as a way to punish Ukrainians for striving to liberate themselves from Russian influence.[24] China's main motivation for its campaign against Taiwan was to exert political deterrence.[25] The wiper attacks occurred weeks before Taiwan's inauguration of a president Beijing did not approve of, and may have been meant to signal to Taiwanese citizens that this would come with costs.[26] Similar non-destructive hacktivist cyberattacks of Chinese origin, with the aim of inducing fear, surfaced during U.S. House Speaker Nancy Pelosi's visit in 2022.[27]

The reason for US destructive behavior is to degrade an adversary's attack capabilities. Based on this goal, the US deployed destructive campaigns against North Korea and Iran to delay their acquisition and deployment of offensive weapons. The underlying motivation behind the US cyber campaigns is threat prevention, both nuclear (Stuxnet) and conventional (attack on Iranian databases). Although the US never officially confirmed its cyber campaigns, former senior US intelligence officials stated that Stuxnet was intended to help the US convince Iran to abandon its pursuit of a nuclear bomb. Similarly, the officials said the attacks against databases were meant to signal that "the United States has enormous capabilities which they [Iran] can never hope to match, and it would be best for all concerned if they simply stopped their offending actions."[28]

The third reason for destructive behavior is retaliation. A case in point is Russia's sabotage of the Olympic games in South Korea. These came after Russian athletes were banned from competing under the Russian flag in the Olympics and receiving medals for their country, due to Russia's systematic manipulation of doping regulations.[29]

Power Dichotomy – The Weak Suffer What They Must

In addition to these commonalities, all cyber campaigns examined took place in a dichotomy. Power asymmetries were extensive. Great powers were able to conduct cyber operations as they felt secure and did not fear any major backlash. Russia, for instance, has not conducted major damaging operations against NATO countries, but it did target the Ukrainian power grid twice in the mid-2010s. The US felt at liberty to go after the nuclear missile programs of both Iran and North Korea, countries that can be situated at the medium and lower spectrum of national power. China, too, was not deterred in its cyber operations against Taiwan.

Leading a crippling campaign against another great power in the cyber domain has most likely not occurred yet, although Washington, Moscow and Beijing may have placed logic bombs in each other's critical infrastructure – malicious code that only activates under certain conditions. The US seems to have taken this path, specifically by planting damaging malware

22 Taiwanese Ministry of Legal Affairs Bureau of Investigation, "Investigation Description of the Incident of Extortion of Important Domestic Enterprises," May 31, 2020, https://web.archive.org/web/20200531005757/https://www.mjib.gov.tw/news/Details/1/607.

23 "Japan's Biggest Port, Nagoya, Hit by Suspected Cyberattack," Nikkei Asia, July 5, 2023, https://asia.nikkei.com/Business/Technology/Japan-s-biggest-port-Nagoya-hit-by-suspected-cyberattack; David E. Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out - *The New York Times*," February 28, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html; WIRED Staff, "Soviets Burned By CIA Hackers? | WIRED," WIRED, March 26, 2004, https://www.wired.com/2004/03/soviets-burned-by-cia-hackers.

24 Centre for Cybersecurity, "The Threat of Destructive Cyber Attacks."

25 Corp, "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware."

26 Corp; Office of the President Taiwan, "Inaugural Address of ROC 15th-Term President Tsai Ing-Wen," May 20, 2020, https://english.president.gov.tw/News/6004.

27 Anne An, "Cyber Tools and Foreign Policy: A False Flag Chinese 'APT' and Nancy Pelosi's Visit to Taiwan," September 29, 2022, https://www.trellix.com/en-us/about/newsroom/stories/research/cyber-tools-and-foreign-policy.html.

28 Valentin Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States," *Journal of Cyber Policy*, August 17, 2018; Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say."

29 Greenberg, "Inside Olympic Destroyer, the Most Deceptive Hack in History."

Destructive great power cyber campaigns outside major conflict*

ATTACKING STATE	SELECTED CYBER UNITS INVOLVED	TARGET COUNTRY	MOTIVATION	SELECTED DESTRUCTIVE EFFECTS
United States (2010–2019)	CIA Clandestine Service's Counter-Proliferation Division	Iran	Degradation of attack capability	Centrifuge destruction, disabling databases
United States (2014–2017)	US Cyber Command and NSA	North Korea	Degradation of attack capability	Failing missiles
Russia (2015–2022)	GRU's Main Centre for Special Technologies	Ukraine	Territorial dispute	Power outages, payment systems affected
Russia (2018)	GRU's Main Centre for Special Technologies	South Korea	Retaliation	Olympic organizer equipment rendered unusable
China (2020)	Ministry of State Security's Winnti Group	Taiwan	Territorial dispute	Corporate payment systems down

*The dates in this table are indicative. US action against North Korea was revealed in 2017 and had been ongoing for years beforehand. Multiple units of various agencies may have been involved in the destructive aspects of cyber operations against Iran between 2010-19. The selected unit in the table pertains to the Stuxnet cyber operation, where the CIA was central in the development of the destructive parts. Regarding BadRabbit malware, there has not yet been a definite attribution to the GRU, despite code overlap with NotPetya. | Sources: Jack Stubbs, "NotPetya Hackers Likely behind Badrabbit Attack: Researchers," Reuters, October 26, 2017, sec. Cyber Risk; James Bamford, "NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar," WIRED, June 12, 2013; United Kingdom, "UK Exposes Series of Russian Cyber Attacks against Olympic and Paralympic Games," GOV.UK, October 19, 2020; Valentin Weber, "Cyberprotection for Critical Infrastructure Resilience: The Case of Taiwan," in Enhancing Resilience In a Chaotic World: The Role of Infrastructure (ISPI, 2023); Sanger and Broad, "Hand of U.S. Leaves North Korea's Missile Program Shaken – The New York Times."

in Russian infrastructure, in response to perceived Russian incursions into critical US systems.[30]

The next section will examine the lessons of past destructive cyber operations for analyzing future damaging operations.

LOCATING THE NEXT BIG DESTRUCTIVE CYBER CAMPAIGN

Beyond renewed destructive operations by the US against Iran and North Korea, China against Taiwan, or Russia against Ukraine, the following great power cyber flares are likely. The US has deployed its most devastating cyber capabilities against non-friendly countries that aim to become nuclear powers. As there are currently no other adversarial states going down this path, such operations against other countries are unlikely. China and Russia, however, will likely be driven by their motives of territorial conquest and retaliation to conduct destructive cyber operations against new targets.

(South) East Asia

China has 17 ongoing territorial disputes.[31] The most likely of these to escalate are those with perceived enemies, such as Vietnam, the Philippines, Japan, and South Korea.[32] With India, too, China might use damaging cyber means, and there are reports that this has already occurred.[33] Because the power dichotomy between India and China is relatively small (both countries have sizeable militaries), and because both are nuclear armed, China's use of destructive cyber power is less likely than in the other border disputes listed above.

30 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid - The New York Times," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

31 Pia Krishnankutty, "Not Just India, Tibet — China Has 17 Territorial Disputes with Its Neighbours, on Land & Sea," *ThePrint* (blog), July 15, 2020, https://theprint.in/theprint-essential/not-just-india-tibet-china-has-17-territorial-disputes-with-its-neighbours-on-land-sea/461115.

32 "Why China Should Be Friendlier to Its Neighbours," *The Economist*, July 4, 2023, https://www.economist.com/briefing/2023/07/04/why-china-should-be-friendlier-to-its-neighbours.

33 Sanger and Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out - The New York Times."

Russia is also involved in several border disputes that could lead to destructive behavior. The spat with Japan over the Kuril Islands (which Russia has been militarizing) has flared up again since Russia's invasion of Ukraine.[34] The Russian assault brought about a shift in thinking in Tokyo, which has increasingly distanced itself from Russia, including in negotiations over the islands.[35]

Caucasus and Southeast Europe

On its southern border, Russia occupies Georgian territory of South Ossetia and Abkhazia. Moscow has also repeatedly led disruptive cyber campaigns against Georgia, e.g., in 2008 and 2019.[36] Moldova, too, has territorial disputes with Russia over Transnistria and has been subjected to Russian cyberattacks.[37] Moscow could extend these to become destructive, since the power dichotomy between Russia on the one hand and Georgia and Moldova on the other is large and because the latter two are not shielded by NATO.

In addition to this, Moscow could retaliate against perceived injustice, as with the cyber operations during the Olympics in South Korea. These activities with retaliatory motives are the most difficult to predict, as Russia is irritated by many international events and not all its retaliatory actions are destructive, but rather disruptive. In addition to this, the Kremlin does not always act upon its threats.[38] What is more, all Olympic games in the coming five years will be held on NATO territory, making destructive Russian attacks in the Olympic context unlikely.[39]

WHAT TO DO

What Should Be Done Against Destructive Cyber Campaigns?

Germany and other EU member countries that champion cyber capacity building at the United Nations ought to increase their capacity building efforts in Ukraine, Moldova, and Georgia. This could be done through existing EU or NATO initiatives or bilaterally to complement multilateral efforts.[40] While Ukraine has done remarkably well in defending its assets in cyberspace, there is always room for more cooperation and (monetary) assistance for Kyiv to further shore up its cyber defenses. Georgia especially appears to have continuous difficulties with DDoS attacks, despite their low sophistication.[41] Tbilisi's preparedness for and resilience to destructive cyber operations is likely to be low. These three countries (Ukraine, Moldova, and Georgia) are the most likely to experience severe Russian cyber campaigns. Further, capacity building should focus on Southeast Asia (Vietnam and the Philippines), where countries will likely experience Chinese destructive cyber activities. With Japan and South Korea, European partners should increase threat-intelligence sharing regarding Russian and Chinese threat actors to more swiftly mitigate potential vulnerabilities.

Second, NATO and EU countries should not change their policies of supporting Ukraine based on Russian threats. Russia has threatened to target arms and humanitarian shipments to Ukraine and by extension, also the countries supporting them. But until now, only cyber disruptions have occurred, not destruction[42] The military strength of the EU/NATO

34 Ike Barrash, "Russia's Militarization of the Kuril Islands | New Perspectives on Asia," Center for Strategic & International Studies, September 27, 2022, https://www.csis.org/blogs/new-perspectives-asia/russias-militarization-kuril-islands.

35 Miki Okuyama, "After Ukraine, Japan Reverts to Old Line on Russian-Controlled Islands," Nikkei Asia, March 10, 2022, https://asia.nikkei.com/Politics/International-relations/After-Ukraine-Japan-reverts-to-old-line-on-Russian-controlled-islands.

36 RFE/RL's Georgian Service, "U.S., U.K. Blame Russia For 2019 Cyberattack On Georgian Websites," *Radio Free Europe/Radio Liberty*, 08:42:48Z, sec. Georgia, https://www.rferl.org/a/tbilisi-washington-blame-russia--cyberattack-georgian-websites/30445595.html; John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008, sec. Technology, https://www.nytimes.com/2008/08/13/technology/13cyber.html.

37 Anastasi Pociumban, "Moldova's Fragile Security Situation | DGAP," DGAP, March 13, 2023, https://dgap.org/en/research/publications/moldovas-fragile-security-situation; Efi Koutsokosta, "Russia Conducting 'Hybrid War' in Moldova with Protests and Cyber Attacks: Prime Minister," euronews, February 8, 2023, https://www.euronews.com/my-europe/2023/02/07/russia-conducting-hybrid-war-in-moldova-with-protests-and-cyber-attacks-prime-minister.

38 Keir Giles, "Putin Is Admitting His Previous Threats Were Hollow by Saying 'This Is Not a Bluff,'" The Guardian, September 21, 2021, https://www.theguardian.com/commentisfree/2022/sep/21/vladimir-putin-previous-threats-ukriane-hollow-bluff.

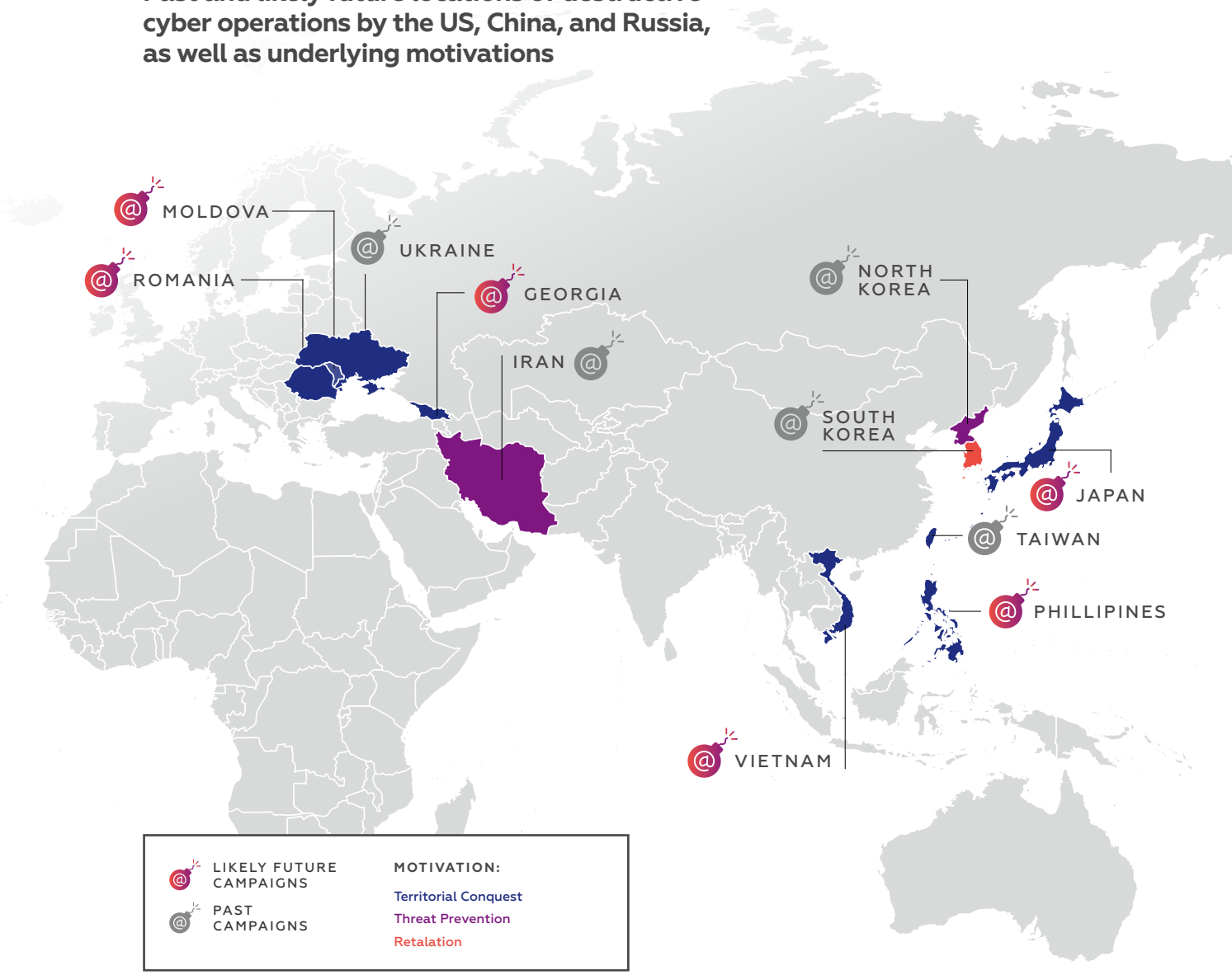
39 "Where Will the Next Olympic Games Be Held?," International Olympic Committee, July 21, 2022, https://olympics.com/ioc/faq/future-olympic-games/where-will-the-next-olympic-games-be-held.

40 Gregorio Baggiani, "The New NATO Cyber Incident Response Center in Moldova," *Nato Defense College Foundation* (blog), June 25, 2021, https://www.natofoundation.org/balkans-black-sea/the-new-nato-cyber-incident-response-center-in-moldova; Council of the European Union, "Moldova: EU Launches Civilian Mission to Strengthen the Resilience of the Security Sector in the Areas of Crisis Management and Countering Hybrid Threats," May 22, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/05/22/moldova-eu-launches-civilian-mission-to-strengthen-the-resilience-of-the-security-sector-in-the-areas-of-crisis-management-and-countering-hybrid-threats.

41 AL JAZEERA, NEWS AGENCIES, "Massive Cyberattack Affects Thousands of Websites in Georgia," October 28, 2019, https://www.aljazeera.com/news/2019/10/28/massive-cyberattack-affects-thousands-of-websites-in-georgia.

42 AL JAZEERA AND NEWS AGENCIES, "Estonia Repels Cyberattacks Claimed by Russian Hackers," August 18, 2022, https://www.aljazeera.com/news/2022/8/18/estonia-says-it-repelled-cyber-attacks-claimed-by-russian-group; Andy Greenberg and Andrew Couts, "2 Polish Men Arrested for Radio Hack That Disrupted Trains | WIRED," September 2, 2023, https://www.wired.com/story/poland-train-radio-attack-security-roundup.

Past and likely future locations of destructive cyber operations by the US, China, and Russia, as well as underlying motivations



Source: Authors own Illustration

vis-à-vis Russia is likely to serve as a powerful deterrent against destructive activities.

Third, the energy sector, and in particular, the electrical grid, should receive a more prominent role in international norm setting, as destructive cyber operations have targeted it the most. While the energy sector, like all critical infrastructure, is already protected by international law, countries should work multilaterally and bilaterally to reduce vulnerabilities in this sector. Regarding the electrical grid in particular, Germany ought to promote an international norm requiring that states refrain from conducting any cyber operations against the electrical grid in peacetime, including cyber espionage operations or the planting of logic bombs.[43] The electrical grid deserves this special protection, as all other critical infrastructure relies on it.

43 Valentin Weber, "How German (Cyber)Diplomacy Can Strengthen Norms in a World of Rule-Breakers," September 26, 2023, https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Ellen Thalman

Layout Lara Bührer

Design Concept WeDo

Acknowledgement
The author is very grateful to Jantje Silomon for commenting on earlier drafts. Any errors are the author's.