Royal United Services Institute
for Defence and Security Studies

Occasional Paper

State Cyberspace Operations

Proposing a Cyber Response Framework

Gary D Brown

State Cyberspace Operations

Proposing a Cyber Response Framework

Gary D Brown

RUSI Occasional Paper, September 2020

Royal United Services Institute
for Defence and Security Studies

189 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, September 2020. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Executive Summary

THE CYBERSPACE THREAT to national security, intellectual property and critical infrastructure has been building steadily for the past two decades, but the military – primarily responsible for the defence of the state – has been slow to respond. The 2008 operation against the US military's classified network by foreign actors served as a wakeup call for national security professionals.

The increased involvement of the military in cyber defence has led to growing concern about cyberspace operations driving states to armed conflict. The primary early effort to address cyber aggression in the existing framework of international law was the UN Group of Governmental Experts (GGE), which was tasked with examining cyberspace. In 2015, it issued a report that showed consensus among its members on a number of cyber norms, but the situation has regressed since then, with the most recent UN GGE focusing on cyber being unable to issue a report at all.

Other efforts to codify or create responsible cyber norms are ongoing, but the current boundaries for appropriate state behaviour in cyberspace are ambiguous, creating a strategically unstable situation with the potential for state cyber operations to lead to unintentional escalation of tension and conflict.

To address this unsatisfactory situation, the author sets out to establish a typology of state cyber operations in order to create a general framework of appropriate responses to cyber aggression.

The paper uses a number of publicly reported cyber incidents to illustrate its central argument. It begins by placing the incidents on a spectrum according to the effects they cause, and then expands the spectrum to also include a ranking according to the target of the cyber operations. The figures used throughout illustrate that using armed conflict as a threshold for response is unsustainable, as state operations normally occur below that kinetically defined level, leaving the appropriate level of response to cyber operations in this 'grey zone' unclear. The figures also make clear that states react differently when they fall victim to cyber operations, even those of a destructive nature, than they do when falling victim to kinetic operations.

The typology of cyber incidents follows from the information included in these figures. However, because state cyber operations are carried out in secret, a good amount of speculation is necessary. The typology is intended to take a middle course between being so broad as to be meaningless and so narrow as to be useless. The result is a relative ranking of incidents by categories of effect and target. Using this ranking, the paper then sets out a proposed set of appropriate responses, again by general category. This approach is somewhat analogous to strategic rules of engagement or a declaratory policy.

States have been reluctant to detail how they would respond to certain cyber operations, fearing that too much detail would encourage adversaries to drive operations right to the line and stop. The paper proposes that being straightforward about what type of cyber responses are appropriate to which types of cyber incident could strike the balance between clarity and ambiguity. This would be enough information for adversaries to signal areas that require extra caution, without allowing operations to become perfectly calculated to avoid engendering a response.

Finally, the paper maps known cyber incidents against the framework to illustrate what cases might be considered to be in which category.

The hope is that establishing a general framework will stimulate discussion among states about appropriate norms for cyberspace. Recognising the reality of states conducting cyberspace operations – and the equal reality that states will, at some point, feel compelled to respond to cyber aggression – setting guidelines and expectations for states on both sides of the equation will help prevent miscalculation and escalation of tension or conflict.

Introduction

AFTER A SLOW, 20-plus-year buildup, military cyber operations suddenly became a hot topic in 2008. As late as 2007, there was no mention of the cyber threat to US national security in the director of national intelligence's public 'Annual Threat Assessment'.[1] The civilian sector was responding to the growing cyber threat long before that. Ironically, starting in the early 1990s, it was warnings of a possible 'cyber Pearl Harbor' that spurred civilians to action.[2] The military was apparently unmoved by the analogy.[3] However, after the US Department of Defense (DoD) discovered its classified computer network had been penetrated and infected with malware, it realised the time had come to put its cyber house in order.

The 2008 case, later dubbed 'the most serious breach of the U.S. military's classified computer systems',[4] was the result of an infected flash drive being inserted into a US military laptop at a base in the Middle East. The malware then spread through thumb drives and other removable storage media to infect both unclassified and classified systems.[5] The malware, known as Agent.btz, ultimately burrowed itself into systems and then beaconed, or called out to, a set internet address to report its successful penetration.[6] When news of the Agent.btz attack was reported in November 2008, it was referred to as 'the worm that ate the Pentagon'.[7] William J Lynn referred to it as both a 'turning point' and 'an important wake-up call'.[8]

As an immediate effect of realising flash drives presented a significant vulnerability, the DoD launched Operation *Buckshot Yankee* and banned removable media from its computer systems.[9] That operational tweak was much less significant than the organisational changes that soon followed.

---

1. John D Negroponte, 'Annual Threat Assessment of the Director of National Intelligence', 2007. By 2012, the director of national intelligence had started ranking cyber as the number one threat.
2. Adam Stone, 'How Leon Panetta's "Cyber Pearl Harbor" Warning Shaped Cyber Command', *Fifth Domain*, 30 July 2019.
3. James Andrew Lewis, *Rethinking Cybersecurity: Strategy, Mass Effect, and States* (Washington, DC and Lanham, MD: CSIS and Rowman & Littlefield, 2018), p. 27.
4. Kim Zetter, 'The Return of the Worm That Ate the Pentagon', *Wired*, 9 December 2011.
5. Noah Shachtman, 'Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack', *Wired*, 25 August 2010.
6. Karl Grindal, 'Operation BUCKSHOT YANKEE', in Jason Healey (ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna: Cyber Conflict Studies Association, 2013).
7. Blake Stilwell, 'The Worst Cyber Attack in DoD History Came from a USB Drive Found in a Parking Lot', *The Mighty*, 27 November 2019.
8. William J Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* (Vol. 89, No. 5, September/October 2010), pp. 97–108.
9. Jennifer H Svan and David Allen, 'DOD Bans the Use of Removable, Flash-Type Drives on All Government Computers', *Stars and Stripes*, 21 November 2008. See also James P Farwell, 'Industry's

In 2010, the DoD combined its cyberspace offence and defence functions into a single military command – US Cyber Command.[10] Kicking the can on determining how a fully independent cyber command would integrate with military and cyber intelligence operations, the DoD co-located Cyber Command with the National Security Agency (NSA), home to an estimated 35,000–55,000 employees.[11] This added the authority and responsibility of leading the new entity to the already full plate of the NSA director.[12]

The creation of US Cyber Command drove a flurry of activity. Not only did many other states subsequently decide they needed cyber commands, but the international law and diplomacy discussions around cyberspace issues revved up.[13] There was heightened interest in the UN Group of Governmental Experts (GGE) dealing with cyber issues.[14] NATO's Cooperative Cyber Defence Centre of Excellence in Estonia hosted a group of international law experts, who wrote the first cyber law manual, the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, and aggressive cyber activities regularly headlined the news.[15] Simply put, there was interest in preventing cyber operations from getting out of hand.[16]

The high point for optimism about controlling aggressive state cyber activity was 2015, when the UN Cyber GGE put forward a list of cyber norms of behaviour that were agreed to by the states participating in it.[17] Among other things, the norms noted that states should not: knowingly

---

Vital Role in National Cyber Security', *Strategic Studies Quarterly* (Vol. 6, No. 4, Winter 2012), pp. 10–41.

10. US Cyber Command, 'U.S. Cyber Command History', <https://www.cybercom.mil/About/History/>, accessed 10 August 2020.
11. Elias Groll, 'By the Numbers: The NSA's Super-Secret Spy Program, PRISM', *Foreign Policy*, 7 June 2013.
12. The decision to dual-hat the positions has continued to bedevil the command. Despite the heroic efforts of the officers filling the positions, it is an incredibly big and challenging job to run two cyber organisations with sometimes divergent strategic interests. United States Government Accountability Office, 'Defence Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened', Report to Congressional Committees, GAO-17-512, August 2017.
13. Not all states disclose the status of their cyber forces, and not all define their collection of cyber capabilities as cyber commands. That said, in 2010 there was one cyber command in the world, and by 2018 there were at least eight others in NATO. See Piret Pernik, *Preparing for Cyber Conflict: Case Studies of Cyber Command* (Tallinn, Estonia: International Centre for Defence and Security, 2018).
14. The full name is the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.
15. Michael N Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
16. The highest-profile example being Stuxnet, discussed below.
17. Member states of the 2015 cyber GGE were all five permanent Security Council members and Belarus, Brazil, Colombia, Egypt, Estonia, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, and Spain. See UN General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International

allow their territory to be used for 'internationally wrongful' cyber acts; conduct or knowingly support cyber activity that intentionally damages critical infrastructure; conduct or knowingly support activity to harm the information systems emergency response teams (CERT/CSIRTS); or use their own emergency response teams for malicious international activity.[18] However, optimism about further progress was shortlived. The next iteration of the UN Cyber GGE in 2017 could not reach consensus on a report, much less build on the ideas put forward in 2015.[19]

The lack of state consensus on applicable norms has not, however, limited the expansion of cyber operations into new and creative areas, some of which are discussed in detail in this paper. Many of these new areas of operations particularly affect civilian populations and are often conducted outside the context of armed conflict. This puts these operations beyond the reach of the heavy restrictions that international humanitarian law (IHL) imposes on state activities affecting civilians during armed conflict.[20] Since state cyber activities are often not easily addressed under existing bodies of law, sub-armed conflict cyber activities operate outside the meaningful application of any legal system. Some state officials nevertheless argue that existing international law can be interpreted to cover such activities sufficiently.[21] Still, the lack of formal guidance coupled with the ambiguity in the evolving domain of cyberspace has created an inherently unstable strategic situation.

This paper develops and presents a theoretical framework for state cyberspace operations. It argues that such a framework, establishing categories of incidents and possible responses, could be helpful in avoiding a cyberspace incident that unintentionally drives states to wage and engage in armed conflict. States with significant strategic cyber capabilities have been reluctant to discuss these issues, leaving most of the public debate to people with little actual knowledge

---

Security', A/70/174, 22 July 2015, <https://undocs.org/A/70/174>, accessed 4 August 2020. The norms recommended included that: states should not knowingly allow their territory to be used for internationally wrongful acts using cyber systems, nor conduct or knowingly support cyber activity that intentionally damages critical infrastructure; states should not conduct or knowingly support activity to harm the information systems of another state's cyber emergency response teams and should not use their own teams for malicious international activity; and states should cooperate in investigating cyber crime and sharing information about cyber vulnerabilities. See also Cooperative Cyber Defence Centre of Excellence (CCDCOE), '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law', <https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/>, accessed 4 August 2020.

18. CCDCOE, '2015 UN GGE Report'.
19. Elaine Korzak, 'UN GGE on Cybersecurity: The End of an Era?', *The Diplomat*, 31 July 2017.
20. International humanitarian law is also referred to as the law of armed conflict.
21. See, for example, Jeremy Wright, 'Cyber and International Law in the 21st Century', speech given on 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accessed 4 August 2020; Chris Borgen, 'Harold Koh on International Law in Cyberspace', *Opinio Juris*, 19 September 2012, <http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace>, accessed 4 August 2020.

of state cyberspace operations. The proposed framework would give decision-makers the opportunity to think through possibilities and effects so that they can avoid tripping into war.

The paper first examines a few significant, representative state cyber activities and responses. Using those as examples, it creates a typology of state cyber activities. It then establishes broad categories of possible state cyber responses. Finally, based on the limited examples in the public record and educated estimation, it provides a sample framework for state cyber responses, matching types of cyber incidents with categories of possible responses, in an effort to provide some guidelines for states wishing to avoid unintentional escalation of tensions.

There are, of course, other ways to increase cyber stability and security. The most successful approaches may turn out to be technology based and led by the private sector. The setting of international cyber security standards by and for private companies is already underway and offers another source for the development of norms.[22] This paper adopts an international relations-based approach to cyber stability, concentrating on the development of international norms applicable to state-sponsored cyber operations. The idea, as fleshed out below, is that states would announce the adoption of a framework similar to the one presented in this paper to clarify what they would consider an aggressive cyber action that would provoke an aggressive response. It would also establish boundaries for appropriate responses to more quotidian state cyber behaviour.[23]

While the approach set out here builds on some extant sources, it also differs from two oft-cited lines of reasoning: that state competition in cyberspace will never result in kinetic warfare, and that it is quite similar to state competition in the nuclear arena, particularly on the issue of deterrence.[24] This paper concurs with scholars who argue that states seem most comfortable responding to cyber aggression with cyber, rather than kinetic, operations (when they respond at all).[25] However, it is likely too early in the development of cyber strategy and capabilities to ignore the possibility that a misstep or miscalculation by a capable state actor in cyberspace could result in an unintentionally escalatory operation that could, in turn, lead to an aggressive response.

---

22. See, for example, Global Commission on the Stability of Cyberspace, <https://cyberstability.org/about/>, accessed 24 August 2020; Siemens, 'Time for Action: Building a Consensus for Cybersecurity', <https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html>, accessed 24 August 2020.
23. This would be consistent with the current agreed competition between states in cyberspace. See Michael P Fischerkeller and Richard J Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *Cyber Defense Review*, 2019.
24. See Thomas Rid, *Cyber War Will Not Take Place* (New York, NY: Oxford University Press, 2013); Sarah Kreps and Jacquelyn Schneider, 'Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics,' *Journal of Cybersecurity* (Vol. 5, No. 1, 2019), pp. 1–11.
25. Henry Farrell and Charles L Glaser, 'The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine,' *Journal of Cybersecurity* (Vol. 3, No. 1, March 2017), pp. 7–17.

The framework set out in this paper encourages states to set rational standards and then follow them. The author based the framework on his experience in cyber operations and US national security, as well as on a review of existing literature on reported cyber incidents and those few times when states have taken actions in cyberspace in an observable manner. In relation to cyber issues, it has seemed that what states negotiate in public and what they do in private are different matters.[26] This paper suggests that states should drop the pretence and simply declare how they plan, in a rational manner, to act and respond to cyber operations to which they fall victim.

26. Because state cyber operations are difficult to attribute, states are able to avoid addressing disconnects between their public statements and their secret actions. See Kenneth Geers et al., 'World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks', FireEye, 2014, <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>, accessed 4 August 2020.

I. Illustrative Case Studies

THE PAPER USES several case studies drawn from the public record to illustrate the issues presented and the proposals offered. Each case study is introduced in conjunction with the discussion of an issue the case demonstrates particularly well.

The case studies should, however, be viewed with caution. Riffing on Clausewitz, it sometimes seems that everything in cyberspace is easy, but nothing is simple.[27] That is, skilled hackers, given enough time, can penetrate almost any system, but the discovery, analysis, attribution and attendant tasks often leave victims perplexed. The cases discussed here have been the subject of endless debate and disagreement over attribution and the precise technical details. With that in mind, the examples are not offered for precise truth but merely as illustrations of situations and possible future expectations. Even with imperfect information, the hope here is that categorising malicious cyber events and observing what evidence exists of states' subsequent reactions – or inaction – may shed light on what cyber activities states would consider to cross the threshold to warfare. This, too, is not as straightforward as it sounds, because states' views on cyber warfare seem to differ from those on traditional, kinetic warfare. Most often, the reaction of victim states to destructive cyber activity has been surprisingly mild, while at times reactions to events that fall far short of destruction, and may not even be clearly unlawful, have been more severe. One illustration of the different reactions to cyber and kinetic events is the alleged Russian cyber attacks on the Ukrainian power grid, described below.

Ukraine

Russia has reportedly launched a number of cyber attacks against Ukraine in the wake of its invasion and annexation of Crimea. *Wired* suggests Russia uses Ukraine as a testbed to perfect its ability to leverage its considerable cyber capabilities to advance its strategic interests.[28] The Ukrainian electric grid has been a favourite target of Russian hackers.[29] Power grid disruption is particularly difficult for civilians because, although an affected portion of the grid might power both civilian and military systems, military systems are often more robust in the face of an attack, leaving civilian systems powered by electricity (in other words, almost all civilian systems) particularly vulnerable.[30] In the absence of a cyber capability, states generally only

27. 'Everything is very simple in war, but the simplest thing is difficult' (Carl von Clausewitz, *On War*, <https://www.clausewitz.com/readings/OnWar1873/BK1ch07.html>, accessed 4 August 2020).
28. Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar', *Wired*, 20 June 2017.
29. *BBC News*, 'Ukraine Power Cut "Was Cyber-Attack"', 11 January 2017.
30. International Committee of the Red Cross (ICRC), 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting, 14–16 November 2018, p. 6, <https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf>, accessed 4 August 2020.

have kinetic means to take power grids offline when they deem it advantageous to do so.[31] Using kinetic means to damage elements of a power grid would be an armed aggression in violation of international law, unless as part of a UN-approved operation or an action in self-defence.

Because disruption of the power grid and other critical infrastructure is particularly devastating for the civilian population, states should expect an increased level of response to incidents affecting critical systems. The lack of evidence of a Ukrainian response in this case may be due to its inability to deliver an effective riposte, and it is also possible that Ukraine responded to the cyber disruption in a non-cyber way.

German Steel Mill Attack (2014)

A confirmed, state-sponsored cyber attack that resulted in significant physical damage to equipment occurred at a German steel mill.[32] In 2014, employees working at an unnamed steel mill were targeted with spear phishing emails containing an attached document or downloadable file with malicious code.[33] The malicious code provided the hackers with remote access into the system. Once the hackers were inside the mill's network, it is unclear exactly what occurred. What is known is that the hacking ultimately led part of the mill's industrial control system to malfunction, which in turn resulted in the inability of a blast furnace to shut down properly. The consequent physical damage to the furnace was characterised as 'massive'.[34] Fortunately, no workers were present and there were no reported injuries.

---

31. *Ibid.*, p. 36.
32. This paper considers cyber operations undertaken by non-state actors sponsored or actively encouraged by states to be state activities conducted by proxies. There is a legal standard for determining when a state is responsible for non-state actors, but it is a difficult test to apply in the cyber context, and some states – most notably Russia – have been especially adept at dancing on the head of this particular pin. See Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA Analysis & Solutions, March 2017, <https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf>, accessed 24 August 2020; US Army Special Operations Command, '"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014', <https://www.hsdl.org/?view&did=815183>, accessed 24 August 2020. A detailed discussion of the applicable legal standard is beyond the scope of this paper, but may be found in Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, pp. 94–100.
33. Spear phishing is 'a targeted attempt to steal sensitive information ... from a specific victim [by] acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online [and then posing] as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging'. See Nena Giandomenico, 'What is Spear-Phishing? Defining and Differentiating Spear-Phishing from Phishing', *DataInsider*, 24 October 2019.
34. Robert M Lee, Michael J Assante and Tim Conway, 'ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper: German Steel Mill Cyber Attack', Industrial Control Systems, 2014, <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>, accessed 24 August 2020; Bundesamt für Sicherheit in der Informationstechnik, 'Die Lage der IT-Sicherheit

Berlin's response to this destruction was muted. As in every case, there may have been a number of reasons for this: uncertainty of attribution; lack of proof tying the actors to the Kremlin; or political considerations. It could also be that the German government responded in non-public ways, either diplomatically or through cyber means.[35] What seems clear is that, had the damage been caused by a squad of Russian *spetsnaz* who clandestinely infiltrated the mill and planted explosives to cause the same damage, the reaction would have been much more intense.

Operation *Cupcake* (2011)

A case illustrating a different aspect of the cyber challenge emerged in 2011. Although the UK has never publicly claimed responsibility for Operation *Cupcake*, MI6 reportedly used a cyber operation to replace bomb-making instructions in an online publication with a recipe for cupcakes.[36] *Inspire*, as it was called, was considered to be Al-Qa'ida's first successful English-language publication.[37]

This case is interesting because of the apparent non-reaction of the state where the magazine's primary editor was living (Yemen) and of the state where the targeted server hosted the digital content. The latter state has not been disclosed but was likely not Yemen because of the paucity of infrastructure there. There is no evidence the state hosting the targeted server, wherever it was, reacted to the incident. This could mean either it was not aware of the operation or simply chose not to respond. It is likely that if a neutral third state hosted a physical printing plant that was targeted for an infiltration by a foreign state to change the contents of a publication, it might have generated a more public response.

These two cases illustrate the difficulty in predicting states' reactions when they fall victim to cyberspace operations. This leaves the international community in an ambiguous, and considerably less stable, strategic situation when it comes to state cyber activities.

---

in Deutschland 2019', <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=E6738510513313529DBBC006229F197A.1_cid503?__blob=publicationFile&v=7>, accessed 4 August 2020.

35. These caveats apply to the other examples given in the paper as well.
36. Duncan Gardham, 'MI6 Attacks Al-Qaeda in "Operation Cupcake"', *The Telegraph*, 2 June 2011; Elizabeth Flock, 'Operation Cupcake: MI6 Replaces Al-Qaeda Bomb-Making Instructions with Cupcake Recipes', *Washington Post*, 3 June 2011.
37. Marc Ambinder, 'So Is It an Inspired Parody?', *The Atlantic*, 1 July 2010.

II. A Spectrum of Cyber Operations

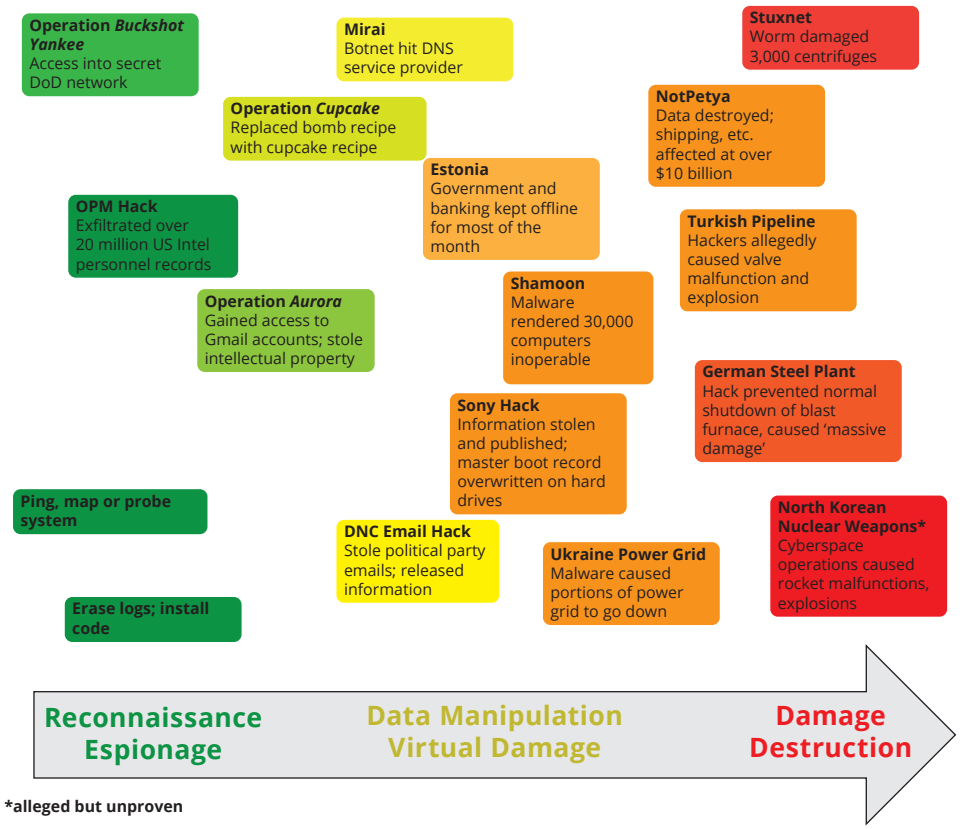
INCREASING CERTAINTY AROUND cyberspace actions and reactions would help stabilise the strategic situation in international relations. In that regard, knowledge of which types of cyber operations might be considered overtly aggressive by states, which would likely be considered acceptable state operations, and which are somewhere between, would be useful. The goal is not necessarily consensus, although that would not be unwelcome. The idea is to arm states with the knowledge of what kind of reaction to expect when planning and executing cyber operations. This would both improve the opportunity for states to signal for diplomatic purposes with more confidence and ensure their peacetime cyber operations remain below the threshold of armed conflict.

One challenge is that there is no consensus on when cyber activities cross the mystical threshold and trigger armed conflict. In the case of kinetic military activities, it is fairly straightforward to conclude in the case of an invasion or a bombing campaign by and between states, for example, that an armed conflict exists. However, even in the kinetic context, there is no authoritative definition of armed conflict.[38] Lacking any state practice to use as a guide, for the purpose of the discussion here, cyber operations would initiate hostilities (an armed conflict) if they cross a clear threshold of violence. That is, cyber operations that result in injury or death to persons, or damage or destruction to objects, would be sufficient to cross the armed conflict threshold.[39] Cyber operations crossing this injury/death/damage/destruction threshold will be referred to in this paper as cyber attacks.

The unclear line dividing peace from war does little to help states avoid accidentally undertaking cyber actions that could be perceived as triggering armed conflict. Providing some framework for discussion about limits other than this nebulous concept should lead to a more predictable and stable international situation. Figure 1 puts publicly reported cyber incidents on a spectrum from least to most aggressive to demonstrate the range of cyber actions that states are taking. This is the first step in a discussion of finding more effective ways to view the issues surrounding cyber aggression.

38. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 80(2), p. 375.
39. The issues surrounding cyber hostilities are discussed extensively in *ibid.* See Rules 82 and 92, and the accompanying commentary, pp. 379–85, 415–20.

Figure 1: Spectrum of Cyber Operations by Effect



Source: Author generated.

Some of the more notorious events from Figure 1 are set out below.

Sony Hack (2014)

The cyber operation carried out against Sony Pictures in 2014 is considered to be the first major state-sponsored destructive cyber attack against a company inside the US.[40] Although most of the attention at the time of the incident was focused on the theft of intellectual property and the release of private data and emails, a contemporaneous FBI description of the attack indicated

40. Andrea Peterson, 'The Sony Pictures Hack, Explained', *Washington Post*, 18 December 2014.

the malware used was capable of overwriting all data on hard drives, including the master boot record (MBR).[41] In the end, about 3,000 of Sony's computers were effectively destroyed.[42]

The US government rather quickly attributed the Sony attack to North Korea, although others expressed uncertainty about the identity of the actors responsible.[43] One reason that North Korea was suspected is that at Christmas that year, Sony intended to release the movie *The Interview*, a comedy about two journalists recruited by the CIA to assassinate North Korean leader Kim Jong-un. North Korea had publicly complained about the film before the hack.[44]

Because of the destructive effects of the operation and the apparent certainty as to the perpetrator, there was some expectation that the US would characterise it as a use of force equivalent to a non-cyber incident with similar effect.[45] In the end, however, the Obama administration called the Sony hack an act of 'cyber vandalism'.[46] This may illustrate the importance of the target in states' response calculus. Had Pyongyang carried out a similar destructive cyber attack against a US military or national security target, it seems unlikely Washington would have been so mild in its reaction.

41. Jim Finkle, 'Exclusive – FBI Warns of "Destructive" Malware in Wake of Sony Attack', *Reuters*, 2 December 2014. The master boot record (MBR) is the file that records where data is located on the hard drive. Without a MBR, it is exceedingly difficult – not quite impossible – to access otherwise intact data on a hard drive. Because of the expense and time involved in attempting to recreate the MBR, hard drives with corrupted MBRs are normally considered destroyed and the data lost.
42. Fred Kaplan, 'Sony Hack: Computer Passwords Included "12345" and "ABCDE"', *Hollywood Reporter*, 2 March 2016.
43. Peterson, 'The Sony Pictures Hack, Explained'.
44. Justin Wm Moyer, 'Why North Korea Has Every Reason to be Upset About Sony's "The Interview"', *Washington Post*, 16 December 2014.
45. See, for example, Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', *Journal of National Security Law & Policy*, 2016, <https://jnslp.com/wp-content/uploads/2017/10/The-2014-Sony-Hack-and-the-Role-of-International-Law_2.pdf>, accessed 24 August 2020; Michael B Kelley and Armin Rosen, 'The US Needs to Stop Pretending the Sony Hack is Anything Less Than an Act of War', *Business Insider*, 15 December 2014.
46. Steve Holland and Doina Chiacu, 'Obama Says Sony Hack Not an Act of War', *Reuters*, 22 December 2014. The US publicly announced economic sanctions in response and denied responsibility for the problems with the North Korean power grid that popped up around the time the US attributed the Sony hack to North Korea. See Ellen Nakashima, 'Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea', *Washington Post*, 14 January 2015. Although the broad definition of critical infrastructure in the US would include Sony as a communications entity, it does not seem that every component of 'critical infrastructure' is treated the same, which confuses matters even more. See also Cybersecurity and Infrastructure Security Agency (CISA), 'Critical Infrastructure Sectors', 24 March 2020, <https://www.cisa.gov/critical-infrastructure-sectors>, accessed 4 August 2020.

Democratic National Committee Hack (2016)

In July 2016, hackers said to be affiliated with the Russian government began a campaign to infiltrate the email servers used by the Democratic National Committee (DNC).[47] As is the case with many serious cyber security breaches, the hackers found penetrating the system fairly easy using spear phishing. The DNC had hired a cyber security company to help secure their systems because they were aware that they were a possible target for foreign state hacking but chose to defer addressing the serious cyber security issues the firm disclosed.[48]

After conducting the hack, the agents responsible provided over 20,000 emails and other documents to WikiLeaks, the website devoted to hosting leaked government and corporate secrets.[49] Some assess that the release of the information had the effect of swinging the US presidential election in favour of Donald Trump.[50]

Although closely aligned with the US political process, the DNC is a private organisation. The result of the operation was the exfiltration of information – the hack itself was unremarkable.[51] The significant diplomatic response from the US was an indication of how important it considered the target, not how seriously it considered the hacking incident itself, which illustrates the importance of targets in states' assessments of cyber aggression.[52]

NotPetya (2017)

Perhaps the most destructive cyber operation ever, NotPetya (named because of its resemblance to a different malware programme, Petya, that surfaced in 2016) attempted to encrypt data and corrupt or delete MBRs on systems it infected.[53] NotPetya was particularly devastating because of the speed at which it spread and its effectiveness. It exploited a vulnerability in the Windows operating system using a leaked NSA programme, and also used a password-stealing

47. Ellen Nakashima and Shane Harris, 'How the Russians Hacked the DNC and Passed its Emails to WikiLeaks', *Washington Post*, 13 July 2018.
48. David E Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York, NY: Crown, 2018), pp. 171–75. The cyber security firm informed the DNC that its employees had barely received any training on avoiding spear phishing, had no capability to anticipate attacks or detect suspicious activity on their network, and overall provided less sophisticated security than Google provides ordinary Gmail users.
49. Jonathan Fildes, 'What is Wikileaks?', *BBC News*, 7 December 2010.
50. Sanger, *The Perfect Weapon*.
51. Eric Lipton, David E Sanger and Scott Shane, 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *New York Times,* 13 December 2016.
52. *Washington Post*, 'Read Mueller Probe Indictment of 12 Russians for Hacking Democrats', last updated 22 March 2019.
53. Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.

programme developed in France.[54] Together the two created a dramatic operation. Most of the victims were based in Ukraine, but NotPetya had global effects, costing an estimated total of $10 billion in damages to international corporations including Maersk, Merck and FedEx.[55] The effects were serious enough that some insurance claims for damages were denied based on the insurance company's assessment that NotPetya constituted an act of war, meaning resulting claims were not covered. The case remains in litigation.[56]

The NotPetya incident has been attributed to Russia.[57] The target appeared to be Ukraine, and it is not clear whether the expansive effects on international corporations were intended or merely a result of recklessness. It is possible that, had the targets affected in Ukraine been related to strategic or national security, the reaction would have been more aggressive.

54. *Ibid.*
55. John Leyden, 'A Year After Devastating NotPetya Outbreak, What Have We Learnt? Er, Not a Lot, Says BlackBerry Bod', *The Register*, 27 June 2018.
56. Kevin Townsend, 'Zurich Rejects Mondelez' $100 Million NotPetya Insurance Claim Citing "Act of War"', *SecurityWeek*, 14 January 2019; Dominic Clarke, 'Cyber Warfare and the Act Of War Exclusion – Insurance – Canada', *Mondaq*, 27 March 2020. Few could have foreseen that the critical definition of what constitutes an act of war in cyberspace would be determined by the judge in an insurance case.
57. *BBC News*, 'UK and US Blame Russia for "Malicious" NotPetya Cyber-Attack', 15 February 2018.

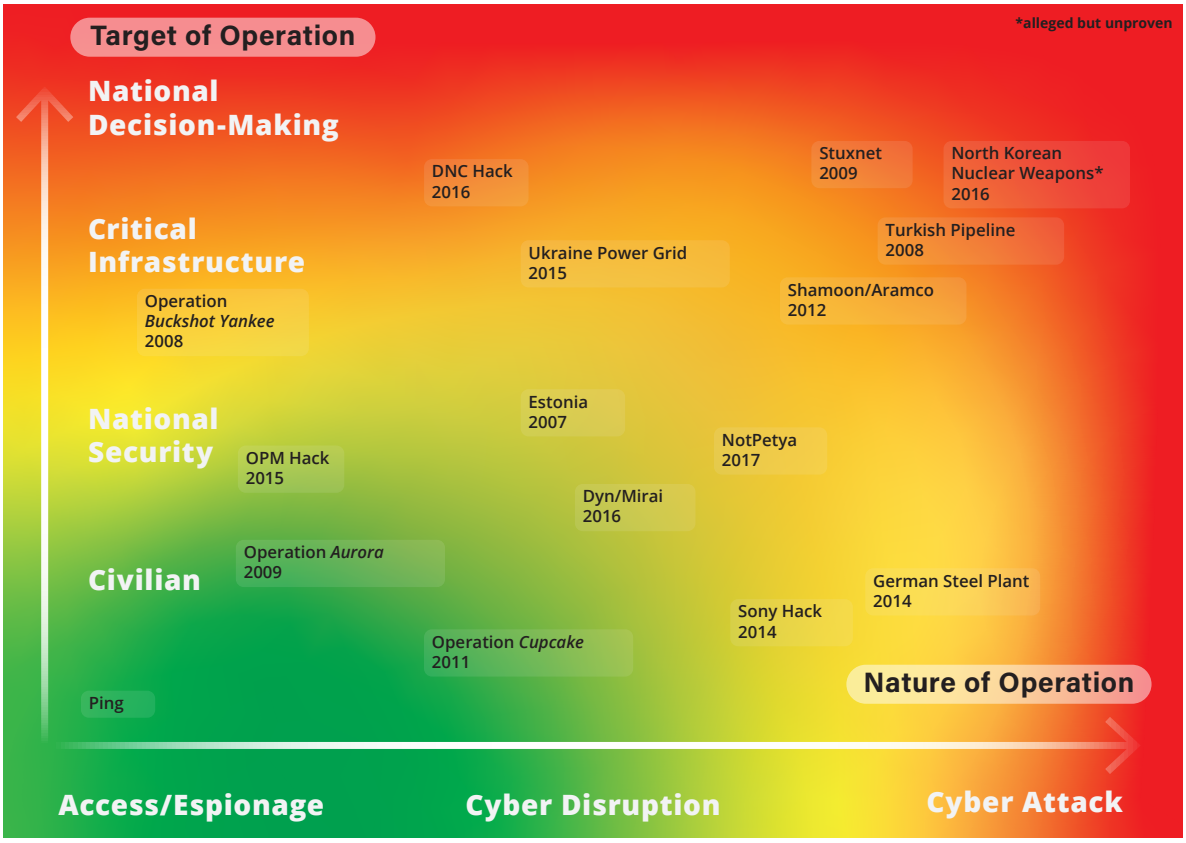
III. The Relative Importance of Targets of Cyber Operations

THE RELIANCE OF the civilian population on internet-connected devices and systems has grown to a degree that could not have been anticipated a generation ago. Similarly, national security and military systems rely heavily on a stable and secure internet – and are consequently exposed to cyber interference and attack. Rather than maintaining the internet as a purely civilian space, states have thus chosen to open a new area of conflict, and the pace and scale of cyber attacks has continued to grow, often in unanticipated ways.

The ubiquity and mixed purposes for which the internet is used is perhaps a major reason why states seem to treat offensive cyber operations differently than they do kinetic offensive operations. State actions and reactions in cyberspace are as attuned to the target of the operation as they are to the effect itself. The modified spectrum of cyber operations below reflects this.[58]

58. The idea for this formulation of the issue was provided by friend and former colleague Andy Metcalf, US Marine Corps Lieutenant Colonel, retired.

Figure 2: Spectrum of Cyber Operations



Source: Author generated.

In Figure 2, the lowest-impact cyber operations – minor effects against low-value targets – are at the bottom left. Opposite, at the top right, are high-effect operations against high-value targets. The graph illustrates how states generally expect and ignore mundane events targeted at low-value assets. On the other hand, although empirical evidence is in short supply, even minor intrusions into the most critical systems might generate aggressive responses.[59] The fact that these effects would be considered armed aggressions if carried out with kinetic means leaves open the possibility that a state might resort to kinetic force in response. This possibility is at the heart of the need for established cyber norms and expectations between states.

The categories in Figure 2 are widely used across different cyber-related contexts. The intended meaning of the category titles in this paper are set out below:

59. States are generally reluctant to share information about cyber operations. When they are the victim, they may not wish to reveal how they know and how much they know, in order to protect their sources. When they are the perpetrator, they may wish to disguise the details of their operations for any number of reasons.

Access operations: Access operations are sometimes called 'enabling operations'.[60] Gaining access to, or penetrating, a targeted system is a prerequisite for most cyber activities, but the access itself is agnostic. It may be used as the first step in an espionage action, an information operation, a disruption or a full-on cyber attack.

Like other cyber operations, access operations must be assessed by their effects. Often, access operations will be stealthy, with the intent of gaining and maintaining access for a period of time without the system owner's knowledge. Such access operations are unlikely to cause damage or destruction. However, it is conceivable that in certain circumstances cyber operators might cause damage or destruction to a system to facilitate an access operation. For example, a secure communications system could be destroyed with cyber means for the purpose of forcing the use of a communications system more susceptible to cyber exploitation.[61] In those cases, the fact that an operation is conducted for the purpose of gaining access to a system will not prevent the activity from being considered a cyber attack.

Cyber disruption: Cyber disruption includes actions that interrupt the flow of information or the function of information systems without causing physical damage or injury.[62] This category represents the majority of malicious cyber operations, such as most distributed denial of service (DDoS) events and inferences with data.[63] In many cases, these actions are imprecisely referred to as cyber attacks. They are distinguished here because the word 'attack' has specific meanings in international law and when more minor incidents are included in the category of attack, it clouds the discussion around escalation avoidance. A good illustration of the havoc that can be caused by a cyber operation that falls short of destruction is Mirai.

Mirai (2016)

The Mirai malware that surfaced in 2016 was the headliner among many strains of botnet-facilitating malware that plagued internet users.[64] Botnets are collections of internet-connected devices whose processing power can be used to carry out simple tasks over the internet. They are often used for malicious purposes, such as sending spam email or flooding websites with such a huge volume of requests for data that the website crashes. Botnets are

60. Jim Keffer, 'Next Steps for US Cyber Command After Split with NSA', *Cipher Brief*, 24 March 2017.
61. See Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 172.
62. There is no single accepted definition of this term. The definition used here is from Owen W Tullos and Gary D Brown, 'On the Spectrum of Cyberspace Operations', *Small Wars Journal*, 11 December 2012, <https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>, accessed 24 August 2020, which also contained the original version of the author's cyber operations spectrum, expanded here.
63. A DDoS attack is a 'malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic'. See Cloudflare, 'What is a DDoS Attack?', <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>, accessed 4 August 2020.
64. Lily Hay Newman, 'The Botnet That Broke the Internet Isn't Going Away', *Wired*, 9 December 2016.

created with malware that compromises the devices of unwitting owners. Simple connected devices, such as webcams and household appliances, that often have weak or no security measures, generally make up the bulk of the bots in botnets. A key element of a successful botnet is acquiring control over a sufficient amount of processing power to make something destructive, profitable or otherwise goal-oriented happen. The Mirai botnet found the 'Internet of Things' to be particularly fertile ground in 2016.[65] The malware lurked on devices, such as routers, webcams and digital video recorders, with little or no practical effect, except that when the individual controlling the botnet chose, the device's computing power could be called upon to become part of a DDoS or other nefarious activity. In this case, the accumulated processing power – 200,000–300,000 devices – was used to help its designers corner a certain market related to the popular online game Minecraft. Unfortunately, a collateral effect was that it also significantly impaired access to Amazon, Netflix, PayPal and Reddit.[66]

Cyber attack: As previously noted, cyber attacks are cyber operations that result in injury or death to persons, or damage or destruction to objects. Perhaps the easiest way to conceptualise how a cyber attack might cause injury or death is to consider any injurious industrial incident, such as an equipment malfunction or failure of a safety system. Modern industrial systems are all controlled by, or at least connected to, computer networks. A cyber attack might cause a system to overpressure, overheat, switch on or off, or perform any number of functions that could directly lead to injuries or deaths. Cyber attacks, because of the observable effects, are the simplest cyber events to categorise.[67] Probably the best-known cyber attack is Stuxnet.[68]

65. '[T]he Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together'. See Matthew Evans quoted in Matt Burgess, 'What is the Internet of Things? WIRED Explains', *Wired*, 16 February 2018.
66. Garrett M Graff, 'How a Dorm Room *Minecraft* Scam Brought Down the Internet', *Wired*, 13 December 2017.
67. A noteworthy outlier here is the DoD, whose doctrine defines cyber attack so broadly that it could include actions as innocuous as standard computer helpdesk activities and remotely rebooting a personal computer, which hardly seem to meet any useful test for cyber attack: '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'. See Joint Chiefs of Staff, 'Cyberspace Operations', Joint Publication 3-12, 2018, p. GL4. However, the DoD has a sometimes uncomfortable relationship with its own doctrine (see, for example, Peter Margulies, 'At War with Itself: The DoD Law of War Manual's Tension Between Doctrine and Practice on Target Verification and Precautions in Attack', in Michael A Newton (ed.), *The United States Department of Defense Law of War Manual: Commentary & Critique* (Cambridge: Cambridge University Press, 2019), and it is unclear in this case that published cyber doctrine has any effect on DoD's cyber operations practice.
68. The event is examined in context in the documentary film *Zero Days* (2016).

Stuxnet (2009)

Stuxnet is the name of the computer worm used to disrupt Iran's uranium enrichment programme. Fearing the uranium was destined to be used in nuclear weapons, it has been reported that the US and Israel jointly developed Stuxnet.[69] This sophisticated malware replicated itself from computer to computer on the internet, activating only on systems running specific Siemens software known to be used in Iran's Natanz uranium enrichment facility. On those systems, Stuxnet looked for other indicators that the system was part of Iran's uranium enrichment programme before it took effect. Eventually, it reached the targeted system and was able to infect programmable logic controllers connected to the sophisticated centrifuges Tehran was using to manufacture enriched uranium.[70] Using the infected logic controllers, Stuxnet altered the spin rates of the centrifuges drastically, but in a manner that was difficult to detect. The extended abuse of the centrifuges destroyed an estimated 1,000 or more of them.[71] Stuxnet continues to be the best real-world example of a cyber attack, although there have been other incidents since then that resulted in the destruction of equipment.[72] In addition, Stuxnet effectively illustrates the intersection of a destructive operation with a highly sensitive target. Leaving aside legitimate concerns about Iran developing a weaponised nuclear capability, the state's uranium enrichment programme is a critical national priority, and when such a priority is cyber targeted, any states responsible for the aggression should anticipate a significant reaction.[73]

The nature of the cyber incident itself only tells part of the story. Since Stuxnet set the bar for what constitutes a cyber attack, there have been other cyber events that resulted in physical destruction, but states' reactions to these events suggest that the target of cyber operations is as important as the character of the cyber operation used. That is, the damaging of a relatively unimportant asset appears to matter less to states than the mere disruption of the functioning of a more sensitive target. This may seem intuitive, but it is a fundamentally different way of viewing the world than the international law governing more traditional state aggression, where the clearest way to escalate to an armed conflict is through the use of destructive or lethal armed force, regardless of the nature of the target.[74]

---

69. William J Broad, John Markoff and David E Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 January 2011.
70. David Kushner, 'The Real Story of Stuxnet', IEEE Spectrum, 26 February 2013; Ralph Langner, 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve', November 2013, <https://www.langner.com/to-kill-a-centrifuge/>, accessed 4 August 2020.
71. Yaakov Katz, 'Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz', *Jerusalem Post*, 24 December 2010.
72. A description of such incidents appears immediately below.
73. See discussion below.
74. This is, at least, the author's interpretation of the meaning of armed conflict. The International Criminal Tribunal for the Former Yugoslavia, in one of its *Tadic* opinions, managed to conclude that 'an armed conflict exists whenever there is a resort to armed force between States'. That this rather unhelpful definition is the best we have would be less disheartening if it had not been adopted by other international bodies after the *Tadic* jurists were forced to come up with something to fill

It also seems states might be more comfortable responding to cyber aggression with non-kinetic actions, such as diplomatic and economic sanctions, or with their own cyber operations. For example, the US responded to the destructive hack on Sony with economic and diplomatic capabilities, as detailed above. Similarly, Iran responded to the Stuxnet attack by increasing its cyber assault on US financial institutions and by launching a cyber attack on Aramco, the Saudi oil company. A final example is the US response to Russia's alleged interference in the US presidential election in 2016, which arguably triggered one of the more serious US cyber reactions that has come to light so far.[75] A traditional international law analysis, largely premised on an examination of the level of violence in aggressive activities, does not seem to be the best predictor of how states will react to cyber threats.

---

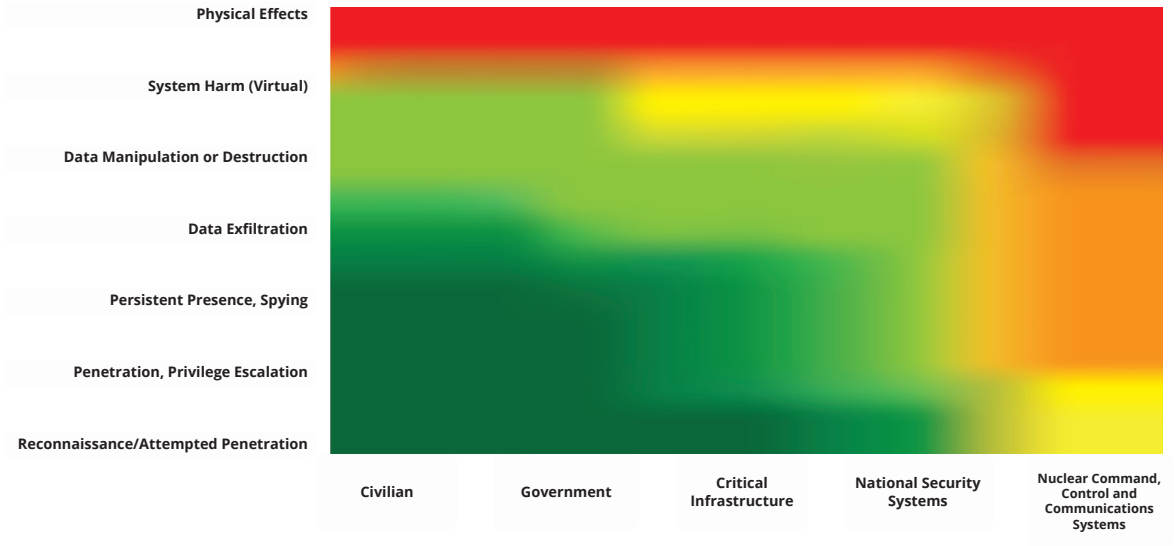
the gap in international law. See Prosecutor vs. Dusko Tadic, 'Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction', ICTY, IT-94-1-A, 2 October 1995, para. 70; ICRC, 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?', ICRC Opinion Paper, 2008.

75. Ellen Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms', *Washington Post*, 26 February 2019. Another indication that the US is becoming more comfortable with cyber responses is the increased offensive cyber authorities the administration reportedly provided to the CIA in 2018. See Zach Dorfman et al., 'Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks', *Yahoo News*, 15 July 2020.

IV. A Typology of Cyber Incidents

USING THE SPECTRUM set out above to assess the seriousness of past cyber incidents, Figure 3 breaks them into broad categories to create a basic typology. The model divides effects on the defender's system into seven categories. Ranked from least to most serious, they are: reconnaissance/attempted penetration; penetration and privilege escalation; persistent presence and spying; data exfiltration; data manipulation or destruction;[76] system harm (virtual); and physical effects.

Figure 3: Typology of Cyber Incidents



Source: Author generated.

The general categories of the *target* of cyber attacks are:

- Civilian systems that are not critical infrastructure.
- Government systems that do not fall into another category.
- Critical infrastructure systems, which can include both government and civilian components.
- National security systems, a category that comprises classified intelligence systems as well as military systems necessary for national defence.
- Nuclear command, control and communications (NC3) systems.

76. Data is not considered an object for purposes of the application of international humanitarian law, so its deletion is not considered equivalent to physical destruction under the model. See Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 100(6), p. 437.

A significant ambiguity with regard to targets is the definition of critical infrastructure. The categories of critical infrastructure vary internationally from state to state, as do its systems. For example, the US defines 16 separate sectors of critical infrastructure – a broad interpretation that may make it easier to define what does *not* meet the definition.[77] For the purposes of this paper, critical infrastructure refers to systems, networks and assets that are so essential that their continued operation is required to ensure the security of the state, its economy and the public's health and safety.[78] This definition is imperfect, but was chosen to create a category limited enough to be meaningful here.

Explanations of the categories of *effects* on targets listed in Figure 3, from least to most serious, are set out below.

Reconnaissance/attempted penetration: Reconnaissance of a cyber system can consist of port scanning and any similar activities. It is often an automated process that aims to simply search for vulnerabilities in systems that may be exploited.[79] State-sponsored hackers would most likely be attempting to find vulnerabilities in particular systems of interest.

Penetration is gaining unauthorised access to a system. At this first level, system administrators may have taken note of aggressors trying unsuccessfully to penetrate the system.

Penetration and privilege escalation: There are a number of ways to penetrate a system without authorisation. To generalise, a system may be penetrated by exploiting people, hardware or software – this paper discusses the latter. The human element is beyond the scope of this paper for several reasons. If the human actor is an insider, counterintelligence will be the focus of the response rather than cyber systems. If they are exploited through social engineering techniques, such as spear phishing, the end result will often be the use of pilfered credentials to gain illicit access, and the cyber analysis does not change based on how the credentials used were acquired.

Hardware exploits involve supply chain issues which are likely to have insider involvement and, in any event, tend to play out over a long period of time, obviating the need for providing direction in advance to deal with rapidly evolving situations.[80] This is beyond the scope of this paper.

A hacker's initial penetration of a system may only provide basic user access to the network. One of the first things successful hackers try to do is escalate their privileges so they can manipulate

77. CISA, 'Critical Infrastructure Sectors'.
78. Margaret Rouse, 'Critical Infrastructure', WhatIs.com, <https://whatis.techtarget.com/definition/critical-infrastructure>, accessed 4 August 2020.
79. Shodan, which might be called an 'Internet of Things' search engine, does this constantly, spotting vulnerable systems. See David Goldman, 'Shodan: The Scariest Search Engine on the Internet', *CNN Business*, 8 April 2013.
80. Christopher A Nissen et al., 'Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War', Mitre, 2018.

the operating system and network configuration, as well as cover their tracks by erasing logs of network activity.[81] Obtaining system administrator privileges is the goal, because that level of access enables them to perform operations in all of the following categories.

Persistent presence and spying: Once a perpetrator has gained access to a system and escalated their privileges, they will want to establish a lasting presence, including a way to re-exploit the system in the event that the penetration is discovered and mitigated. This may include installing malware or creating additional user accounts to provide a way to return, or a backdoor.

Spying, as used in this category, involves 'poking around' in a system to observe how it is configured and what information is located there. As defined here, it will involve some exchange of data packets (because that is simply how the internet works), but no export of data on a larger scale. There is some crossover between this category and data exfiltration.

Data exfiltration: Sending copies of data outside the system might be the conclusion of an espionage-driven activity. All states engage in espionage, and have generally come to accept that their adversaries will do the same.[82] In the case of cyber espionage, an unlimited number of copies of data may be made and sent off the network without adverse impact to the original.[83] It is the possession of the information or knowledge that is the end result of the activity.

Data manipulation or destruction: If a hacker goes beyond copying information and instead uses system access to manipulate, change, or delete information or data, the activity will be categorised as a more serious action and will lead to consideration of more serious responses.

Virtual damage to a system or adversely affecting functionality: The line between virtual and physical damage can be surprisingly blurry. The category of virtual damage is meant to convey the action of a malicious actor causing a system not to function in the intended way but not permanently damaging it. This is similar to when a user, perhaps after loading a new programme or losing internet connectivity, finds their computer frozen and is forced to reboot to return it to operation. If such a situation were caused by an intentional actor rather than by normal noise in the system, it would fall under this category.

Because it can be difficult to articulate the difference between virtual and physical damage, there is some controversy among international law experts.[84] For the purpose of this matrix,

81. Jeff Melnick, 'What Is Privilege Escalation?', Netwrix Blog, last updated 25 March 2020, <https://blog.netwrix.com/2018/09/05/what-is-privilege-escalation/>, accessed 4 August 2020.
82. As noted earlier, cyber activities that constitute espionage are not a violation of international law per se. Espionage is criminalised under domestic law.
83. The interesting discussion of how this differs from theft in the physical world is beyond the scope of this paper.
84. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rules 4(11) and 92(10) document the discussion of the International Group of Experts who drafted the manual regarding the status of cyber operations that limit the functionality of the target system.

loss of functionality is considered to be different from physical damage. Loss of functionality, including situations that require software to be reloaded or firmware to be flashed, falls into this category. If physical components of a system are permanently damaged so that they must be replaced, the operation that caused the effect would be considered to have caused physical damage.

Physical damage or destruction: The most serious situations are the easiest to categorise. If systems must be physically repaired or replaced, the cyber operation leading to that will be in this most serious category of operations.

To the extent the categories align with stages of a cyber operation, categorising them might sometimes be a matter of how quickly an operation is detected.[85] That is, an operation intended to damage or destroy a system, if detected early and thwarted, might only be a privilege escalation incident, because the ultimate goal remained undiscovered. This could be considered a flaw in the approach, but as the framework proposed in this paper is intended to prevent escalation of tension, it is designed to err on the side of caution or under- rather than over-response.

85. DNV.GL, 'The Seven Phases of a Cyber Attack', <https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270>, accessed 24 August 2020.

V. Why a Framework for Cyber Response?

STATE RESPONSES TO cyber incidents are even less well documented than the incidents themselves, so mapping categories of response against incidents is a study in educated guessing. The response matrix below is a product of exactly that. It is meant to be one logical form declaratory rules could take.

A state's response matrix, like the one proposed here, would have both internal and external purposes. Internal to the government, it may be thought of as a guide for developing rules of engagement (ROE) that establish a range of appropriate responses in advance, depending on the level of the triggering incident. It would also help guide the thinking of civilians making decisions that could affect the military. To external audiences, it sets expectations for what kinds of state behaviour in cyberspace will trigger what level of response.

The term 'ROE' is used here to mean guidance provided to operators to permit them to take appropriate actions in ambiguous, developing situations. Military ROE are often thought of as tactical guidance given to fielded forces to ensure their compliance with law and policy.[86] In the US, in the absence of specific guidance, military forces look to the 'Standing Rules of Engagement'.[87] That instruction provides general direction on when to use force and when to exercise the right of self-defence. The way ROE is used in this paper is similar in function to the high-level, general advice in the 'Standing Rules of Engagement'. In addition, the ROE framework discussed here is also similar because it has an external as well as an internal audience. For the US, the publicly released 'Standing Rules of Engagement' serve notice on adversaries of the broad definition of self-defence it provides to its forces, suggesting caution is in order when encountering US forces, even in peacetime. While the cyber ROE proposed here would provide general internal guidance, they are more focused on the external messaging. Their greatest function would be to signal expectations and intent, increasing understanding and decreasing accidental escalation of tension or conflict.

One important note about the way ROE is used in this paper is that it applies to state cyber operations conducted by any actors, not just military forces. States seem to not be overly concerned about what category of state actor carries out which type of cyber operations. In

86. Dustin Kouba (ed.), 'Operational Law Handbook', 17th edition, US Army, 2017, <https://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2017.pdf>, accessed 24 August 2020.
87. 'Standing Rules of Engagement for US Forces', in CJCSI 3121.01B, 13 June 2005, <http://navybmr.com/study%20material/CJCSI%203121.01B%20ENCLOSURE%20(L),%20STANDING%20RULES%20OF%20ENGAGEMENT%20STANDING%20RULES%20OF%20THE%20USE%20OF%20FORCE%20FOR%20U.%20S.%20FORCES.pdf>, accessed 4 August 2020.

China, the People's Liberation Army engages in espionage, Russia leverages cyber capabilities in both its military forces and intelligence services, and the US employs military forces and intelligence agencies in carrying out cyber operations.[88] So, although it is potentially confusing to use the term 'ROE' to refer to a framework for both military and non-military actions, the concept is a good analogy for the kind of general guidance it is meant to provide. Appropriately specific, publicly disclosed ROE would be similar to a declaratory policy.

The peacetime cyber ROE framework sketched out here is concerned with appropriate actions to be taken when responding in cyberspace, but not every state cyber self-defence action requires ROE. In some situations, state cyber operations are identical to the actions of civilian owners and operators. The government, like any system operator, is permitted to use traditional cyber defence actions to secure its networks.[89] Actions like monitoring network traffic, establishing firewalls and deleting malware are referred to as 'cyber hygiene' to distinguish them from more active defence measures.[90]

Because of the inherent uncertainty in cyberspace, crafting cyber ROE is far more challenging than writing ROE for kinetic military operations. Not only do the complex combinations of actors, targets and actions possible in cyberspace defy easy categorisation – as is apparent from the effort above – but it is also difficult to find the sweet spot for response categories. Overly specific guidance would constantly change based on evolving capabilities and systems, and would probably be too sensitive to disclose to the public. Overly general guidance is no guidance at all, a good example being the 2015 DoD cyber strategy, in which the US declared its policy to respond to cyber aggression 'at a time … and place of our choosing'.[91] Such vague warnings fail to provide meaningful clarification to states seeking to avoid unintentional escalation.

The experience of the US military reflects the challenges of crafting rules for cyberspace that are permissive enough to allow for an effective defence, while imposing enough restrictions to avoid

88. Mikk Raud, 'China and Cyber: Attitudes, Strategy, Organisation', CCDCOE, 2016; Michael Connell and Sarah Vogler, 'Russia's Approach to Cyber Warfare', CNA, September 2016; Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms'; Dorfman et al., 'Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks'.
89. C Robert Kehler, Herbert Lin and Michael Sulmeyer, 'Rules of Engagement for Cyberspace Operations: A View from the USA', *Journal of Cybersecurity* (Vol. 3, No. 1, March 2017).
90. For the sake of completion, these actions are included in the framework proposed below.
91. The DoD's 2015 cyber strategy document noted that the US would 'respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law' (p. 9), but that was too vague to provide the direction needed to avoid unintentional escalation. This appears to have been an intentional exercise in strategic ambiguity to avoid disclosing 'red lines' to adversaries, but based on the continuing cyber aggression aimed at the US in its wake, and the more specific statements and responses in the years following, the effectiveness of the vague statement might be questioned. See DoD, 'The Department of Defense Cyber Strategy', April 2015.

unintentionally escalating a situation. Beyond cyber hygiene, military actions in cyberspace have been carefully scrutinised. In particular, permission to engage in sharper defensive action – off the military's own network – in the absence of specific higher-level authority has been controversial.[92] As commander of US Strategic Command (2011–13), General C Robert Kehler was responsible for US military cyber operations. Kehler noted the difference in the defensive actions military units are permitted to take in the kinetic context and in cyberspace:

> [A] military unit experiencing a cyberattack would not be allowed on its own authority to conduct a cyberattack (or kinetic attack, for that matter) against the Ministry of Defense headquarters of the nation believed to be responsible. Such a response would be an overtly offensive action analogous to striking the airfield from which an attacking airplane was launched and would require separate authority.[93]

There is concern that peacetime military cyber actions, if not tightly constrained, might quickly spiral out of control, causing collateral damage and injuries, as well as risking escalation to armed conflict.[94] In addition, kinetic self-defence is favoured because the result of preventing immediate self-defence could easily be observed in death and injury.[95] Constantly giving ground in cyberspace may have disastrous long-term consequences but has not yet resulted in instant casualties. The longer wait for the denouement of cyber attacks seems to have led to an overcautious approach, consequently emboldening adversaries.

Tight restrictions on cyber self-defence actions are in stark contrast to military guidance in kinetic engagements.[96] Military forces, within general guidelines, are allowed to act in self-defence when they are physically attacked. They are not required to seek specific permission before responding in such cases.[97]

The challenges created by overly restricting defensive military cyber actions are shared by other strategic state functions. If every action in cyber self-defence is weighty and requires

---

92. It is challenging, and often fruitless, to attempt to distinguish between offensive actions taken for defensive purposes (defensive actions) and those taken for the purpose of advancing an offensive goal (offensive actions). This confusion is not limited to cyberspace activities; in most kinetic situations, an effective defence requires more than 'duck and cover'. As subjective and unsatisfactory as it is, the intent of the actor drives this distinction.
93. Kehler, Lin and Sulmeyer, 'Rules of Engagement for Cyberspace Operations', p. 71. The article then explains 'active defense'.
94. See Erica D Borghard and Shawn W Lonergan, 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly* (Vol. 13, No. 3, 2019), pp. 122–45.
95. An infamous case of a US military unit failing to act in self-defence is that of the USS *Stark* which, while on patrol in the Persian Gulf, was struck by two Exocet missiles fired by an Iraqi Mirage fighter. The *Stark* never employed its defensive systems, and the missile strikes resulted in the deaths of 37 sailors. See Mark Thompson, 'Those Who Cannot Remember the Past', *Time*, 18 May 2012.
96. Included in the notion of self-defence is acting in defence of others. See 'Standing Rules of Engagement for US Forces', paras. 6(b)(1) and 6(c)(1).
97. See 'Standing Rules of Engagement for US Forces'.

in-depth consideration, it necessitates the collection and analysis of evidence. Even if evidence is available in cases of cyber aggression, by the time it is gathered and presented to senior leaders, the moment to respond will almost certainly have passed. This inbuilt delay results in a strategic gap that could be addressed with standing peacetime cyber ROE.

International law recognises that in some cases there must be a rapid response for the right of self-defence to be meaningful. These parameters were first formulated in the *Caroline* case from 1837, in which self-defence was said to be permissible if the necessity is 'instant, overwhelming, leaving no choice of means, and no moment for deliberation'.[98] The defensive response is also constrained by the same necessity; that is, it is limited to what is necessary under the circumstances for the right of self-defence to be meaningful. The events leading to the *Caroline* case occurred during an armed rebellion (in other words, an armed conflict), but the case's logic can serve as a model for structuring peacetime defensive rules, and in particular the notion that an immediate response may be necessary for a defensive activity to have an appropriate impact.

If states adopt peacetime ROE for cyber, they would only have the status of national policy, or perhaps national law, but not international law. Still, if the primary state cyberspace actors acknowledge and adhere to a framework for cyber operations, it could be the foundation for establishing useful international norms applicable to cyber activities. A shared understanding of appropriate state behaviour in cyberspace would be a stabilising development.

Cyber operations, particularly those undertaken by states capable of advanced and persistent operations, tend to be bespoke, specifically designed for the situation. One factor that has discouraged states from making declaratory policies about cyberspace is the inability to agree on precise categories and definitions. This proposed framework takes a different approach. Like the categories in the incident typology, the categories of possible cyber responses in the framework are broad. Broad categories, although they run the risk of being over-inclusive, at least provide a starting point for a common international understanding of what types of cyber behaviour are more likely to cause an escalation of tensions.

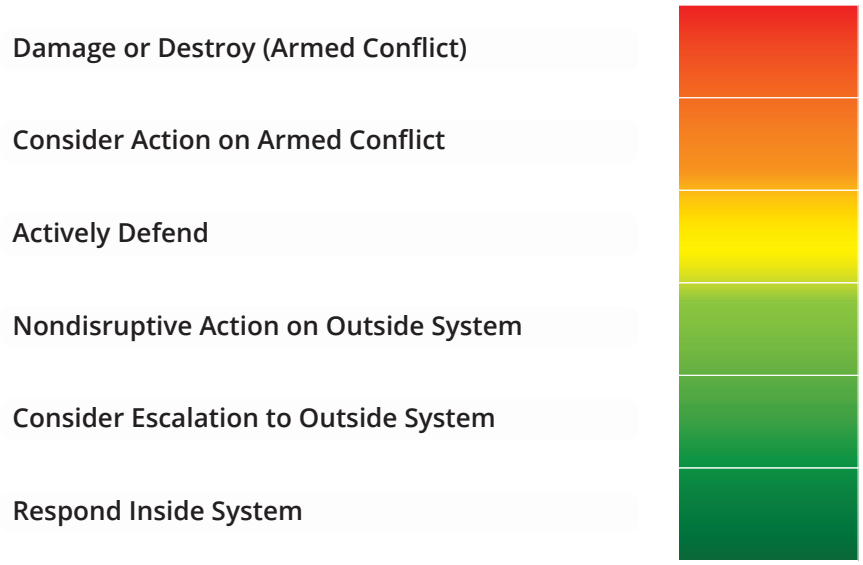
It is important to note that these responses are state activities, and do not include the private actions of citizens, corporations or other entities acting independently of state control.[99]

Framework of Defensive Responses

The framework in this paper divides defensive responses into four broad categories, from least to most serious: response inside the system; reaching outside the system; active hack-back; and physical effects. In addition, there are two 'border' categories.

98. Malcolm N Shaw, *International Law*, 8th edition (Cambridge: Cambridge University Press, 2017), p. 861. A brief summary of the case and additional references can be found in Matthew Waxman, 'The "Caroline" Affair in the Evolving International Law of Self-Defense', *Lawfare*, 28 August 2018.
99. It does include private actors functioning as proxies for the state, regardless of how the state characterises them.

Figure 4: Possible Responses to Cyber Incidents



Source: Author generated.

Response inside the system: These responses are neither confrontational nor controversial – they merely represent taking appropriate measures (as a form of good practice) in the wake of unwelcome activity on a network. They may include cyber hygiene measures discussed previously, such as updating antivirus signatures and patching software. They should also be expected to include hunting within the network. Hunting might, for example, involve network administrators analysing traffic on the network to see if they can identify suspicious patterns of activity, such as multiple logins from different locations using the same user credentials. Network administrators may delete extraneous files, malware and user accounts on the system to protect it. They might also block traffic from suspicious or known malicious IP addresses.

For example, in 2015 the US Office of Personnel Management (OPM) was hacked, resulting in the exfiltration of over 18 million security clearance, personnel and fingerprint files of US government employees and contractors.[100] The penetration was discovered by an OPM system administrator who recognised that outbound network traffic was being directed to a site with a name misleadingly similar to OPM.[101] The security experts called in to address the problem observed the malware at work for some time to collect information on its function, and then used a scheduled power outage at the network centre to disguise their deletion of the malware. Actions such as these are uncontroversial in the wake of discovering malware on a system. The risk of escalation from this type of defensive response is zero.

100. Brendan I Koerner, 'Inside the Cyberattack That Shocked the US Government', *Wired*, 23 October 2016.
101. *Ibid.*

Nondisruptive action on outside systems: More assertive actions against systems may lead defenders to aggressively track malicious activity to its source, deleting malware on machines or networks outside their own network. They could potentially also install non-destructive malware on the source system to track or prevent future aggressions, and delete data at the source of the aggression, particularly data that may have been exfiltrated from the defender's own system. These techniques may require defenders to gain access to outside systems in ways not authorised by the outside system's owner.[102] Defenders would also use that access to gain information helpful in mitigating current and preventing future malicious activities from the source.

For example, in 2012 the Georgian government struck back against hackers who were conducting espionage inside their government computer networks. The Georgian defenders attached malware to documents containing keywords they knew would interest the hackers, and strategically placed the documents in compromised network locations.[103] When the infected documents were exfiltrated onto the hackers' systems, Georgian defenders used the malware resident on the pilfered files to send incriminating documents, as well as photos taken using the hackers' webcams, to the Georgian government so they could identify the perpetrators.[104]

Active defence: The term 'active defence' has been defined in a number of different ways that could apply to defensive activities across all four categories of the response framework.[105] For the purposes of this discussion, active defence includes accessing an aggressor's computer or network without authorisation to disrupt continued unauthorised activity against the defender's

102. Currently prohibited in the US under the 'Computer Fraud and Abuse Act 1986 (US)' (CFAA), 18 USC § 1030.
103. A technique made famous in cyber lore by Clifford Stoll's wonderful narrative, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York, NY: Doubleday, 1989).
104. Graham Clueley, 'Counterattack! Suspected Hacker Caught on HIS WEBCAM, While Spying on Georgia', *Naked Security*, 31 October 2012; Scott Berinato, 'Active Defense and "Hacking Back": A Primer', *Harvard Business Review*, 21 May 2018.
105. For example, one definition of active cyber defence is 'a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets'. See Dorothy E Denning and Bradley J Strawser, 'Active Cyber Defense: Applying Air Defense to the Cyber Domain', in George Perkovich and Ariel E Levite (eds), *Understanding Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017). This broad definition would capture activities in all four categories in the framework proposed in this paper. Further, in the UK system, the term 'active cyber defence' refers to a set of activities developed to reduce national exposure to cyber-criminal activities and does not include the type of cyber activities described here. See also Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, p. 563.

systems or network.[106] All actions here would remain non-destructive, and therefore below what appears to be what states would consider an armed attack.[107]

Actions in this category include disrupting or otherwise non-destructively taking down an aggressor's systems and implanting persistent malware to help prevent future aggression.

In 2018, the *Washington Post* reported that US Cyber Command interrupted the operations of a troll farm in Russia that had interfered in the US presidential election in 2016.[108] US Cyber Command's actions included both network interference and direct messaging to hackers working at the targeted Internet Research Agency. Both of these types of action would fall under this category of response.

Another example in this category is set out in former NSA and CIA Director Michael V Hayden's book, *Playing to the Edge: American Intelligence in the Age of Terror.* Hayden recounts that, in order to prevent distribution of a terrorist propaganda video, the US DoD, perhaps through NSA, took down websites that were to be used to distribute the video. Although he provides few details of the incident, it appears the hacks were effective at ending the distribution of the video during what the US considered a critical period around the anniversary of the 9/11 attacks.[109] On the other side of the equation, there were allegations at the time that the US action also accidentally took down many other, unrelated websites in Saudi Arabia and Germany.[110]

Damage or destroy: A state's use of the highest-level response would indicate it had concluded that the aggressive cyber activity crossed the threshold of a use of force or armed attack and drove the situation to the brink of an armed conflict. At this point, the state could employ high-level cyber capabilities, damaging systems, causing them to malfunction or even be destroyed.[111]

---

106. This language was adopted from the 'Active Cyber Defense Certainty Act', a much-maligned bill introduced in the US House of Representatives in 2017 as a proposed amendment to the CFAA. The criticism focused on the bill's intent to give active defence authority to private actors. See, for example, Tom Kulik, 'Why the Active Cyber Defense Certainty Act is a Bad Idea', *Above the Law*, 29 January 2018. Many of the actions proposed in this framework would be prohibited by CFAA in its current form.
107. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 71(6), pp. 39–44.
108. Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms'.
109. Michael V Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York, NY: Penguin, 2016), pp. 149–50.
110. Ellen Nakashima, 'Dismantling of Saudi–CIA Web Site Illustrates Need for Clearer Cyberwar Policies', *Washington Post*, 19 March 2010.
111. Crossing the threshold here also opens the possibility of kinetic responses with more traditional military means.

There are a number of obvious limitations to the proposed framework, and it is not meant to be a definitive expression of state practice, much less a complete expression of international law – which is in any event unclear in some areas of application to cyber operations. Two particular limitations should be noted. The first is that no distinction is drawn between cyber operations conducted by military forces or organisations and those conducted by members of intelligence services. Although major cyber states have separate cyber forces in each group, often with distinct missions, there are large areas of overlap and the distinctions, while critical in democratic states for protecting domestic civil liberties and the rule of law, are largely irrelevant internationally. A cyber activity's effects drive its characterisation under international law.[112] The unique role of espionage under international law is reflected in the proposed framework and does not rely on the status of the actor.[113]

The other shortfall is the absence of information operations in the framework. Cyber-enabled information operations constitute perhaps the most significant cyber threat to democracy.[114] Peacetime information operations are not adequately addressed under international law and continue to cause great consternation in states worldwide. Unfortunately, state practice and response are even less well developed in that area than they are with regard to other types of cyber operations, and do not yet provide enough information for inclusion here.

112. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 32(6), p. 170.
113. Espionage is not a violation of international law. See *ibid.*
114. Gary Brown, 'Addressing Cyber-Enabled Information Operations', *RUSI Newsbrief* (Vol. 40, No. 4, May 2020).

VI. Applying the Framework

THE PRACTICAL APPLICATION of a general response framework like the one set out here will be challenging because of uncertainty about state responsibility and motivation, as well as diplomatic and political considerations specific to each situation and international relationship. For the most part, these considerations are just part of the background of interstate relations. More powerful states can take more liberties in their activities than smaller ones, for example. States manage to navigate through these uncertainties with some regularity. However, in the cyber context, state responsibility – or what is often referred to as the attribution issue – has been the most vexing.

Uncertainty about the rules of attribution has been a major stumbling block in the development of objective dialogues about cyberspace operations, largely because attributing state responsibility for operations is simply much more challenging in cyber situations than it is in kinetic ones.[115] As discussed earlier, states do play games on the margins of responsibility in kinetic space by using proxy forces, for example. Such manoeuvres may challenge legal standards of responsibility, but as a factual matter kinetic aggression remains relatively easy to tie to the acting state. In the case of cyber operations, even when a state is quite capable of proving attribution, it may be unwilling to share the evidence, because it might disclose intelligence sources, methods or capabilities. With the framework set out here, the author proposes that states are not necessarily required to announce the evidence used to establish responsibility, but would be rather bound by acting within the remit of international law.[116] That may mean providing attribution details in private communications with friendly states, with the state targeted for response, or publicly, depending on the situation. In some cases, it might be reasonable to proceed with a response based on the framework without communicating at all beforehand. The purpose of establishing a menu of possible responses is to provide advance notice to states engaged in cyber operations of what to expect. If a state is choosing a very serious response, such as a kinetic action, in most cases it would seem reasonable (required under international law) to provide some notice and opportunity to respond, but circumstances could dictate otherwise. Most of the response categories outlined here share the useful characteristic of being non-lethal and, for the most part, temporary in effect, which helps mitigate any errors in attribution.

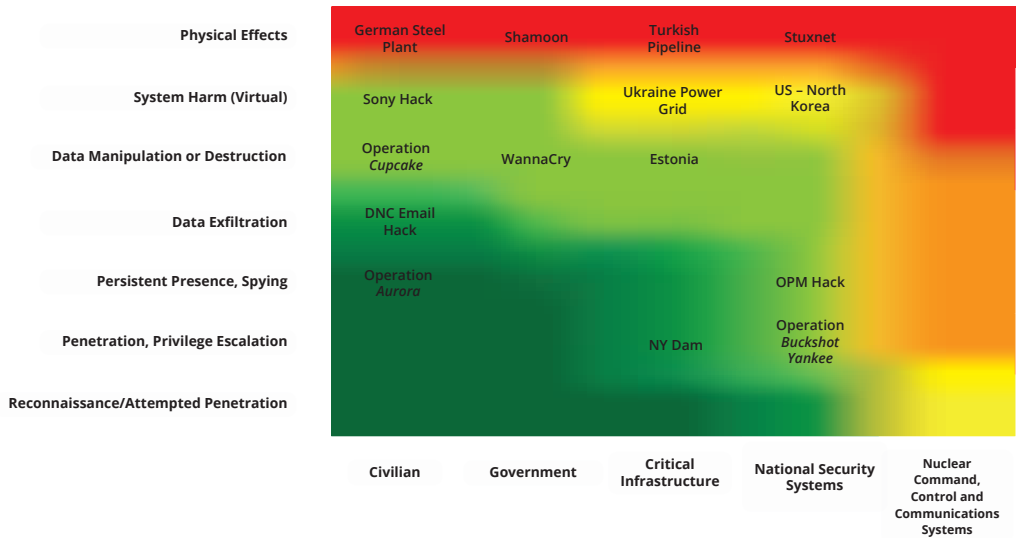
The case studies used below to illustrate how cyber ROE might apply are based on press reporting and the limited response statements made by governments. Inevitably, because the aggressors

115. See, for example, Florian J Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia', *Contemporary Security Policy* (Vol. 41, No. 1, 2020), pp. 55–81.
116. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Chap. 4, Section 1(10), pp. 81–82. Realistically, however, since Iraq in 2003, the political and public pressure to set out this evidence explicitly in the case of a significant response would be high. See *BBC News*, 'Chilcot Report: Tony Blair's Iraq War Case Not Justified', 6 July 2016.

in these cases have generally been silent – and would, in any event, not be motivated to be entirely truthful – some of the facts will be imperfect. The intent is not to establish the absolute truth in each case, but to use the scenario as described to illustrate what activity might generate the responses proposed in the model.

When an operation is considered 'attributed', it is nearly always based on reports from the media or cyber security companies. Although the public record may not have disclosed the facts in perfect detail, it is nevertheless useful to examine actual cyber operations to see what category of response they would merit if the facts are as reported.[117]

Figure 5: Applying the Framework



Source: Author generated.

Examples of the last two categories of activity directed against civilian and government systems occur on a regular basis, conducted by both state and non-state actors. Scanning across the internet for vulnerabilities and basic follow-on activities is accepted as a fact of the modern connected world. These events are not escalatory.

Operation *Aurora* (2009)

Using an infected website to distribute the malware, Operation *Aurora* targeted the Gmail accounts of human rights activists and stole intellectual property, including the source code for Google's search engine.[118] Sensitive counterintelligence data from the US government

117. Cases discussed earlier in the paper are not repeated here.

118. Kim Zetter, 'Google Hack Attack Was Ultra Sophisticated, New Details Show', *Wired*, 14 January 2010.

was also accessed.[119] The group that carried out *Aurora* is said to be affiliated with the Chinese government.[120]

New York Dam (2013)

Using a vulnerability in a cellular modem, hackers reportedly based in Iran broke into the command and control system of a 20-foot flood control dam outside New York City. The hackers would normally have been able to release water from behind the dam, but it was undergoing repairs and its sluice gate had been manually disconnected.[121]

Estonia (2007)

After relocating a statue depicting a Soviet soldier from the centre of Tallinn to a military cemetery, Estonia became the target of a three-week cyber incident. Government, media, financial resources and businesses were all targeted with DDoS. Based on the situation, Moscow's reaction and operational indicators, Russia is considered to have been responsible for the incident. The DDoS caused significant social disruption and economic loss in Estonia.[122] Among other things, bank cash machines went offline, government ministries were unable to conduct business and Estonian media websites were unavailable.[123]

Turkish Pipeline (2008)

Although there are still significant doubts about whether this destruction was caused by a cyber attack, it illustrates what an attack on civilian infrastructure would look like.[124] In the cyber attack version of events, Russians reportedly gained access to the network controlling the pipeline through a vulnerable security camera. Once in the system, they clandestinely increased the pressure of the oil passing through the pipeline, causing the over-pressuring to go undetected until the pipeline ruptured, causing a fire.[125]

---

119. Ellen Nakashima, 'Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say', *Washington Post*, 20 May 2013.
120. Jim Finkle, 'Hacker Group in China Linked to Big Cyber Attacks: Symantec', *Reuters*, 17 September 2013.
121. David E Sanger, 'US Indicts Iranians in Cyberattacks on Banks and a Dam', *New York Times*, 24 March 2016; Mark Thompson, 'Iranian Cyber Attack on New York Dam Shows Future of War', *Time*, 24 March 2016.
122. Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', CCDCOE, <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>, accessed 4 August 2020.
123. Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', *Wired*, 21 August 2007.
124. Robert M Lee, 'Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline', SANS, 15 June 2015.
125. Ariel Bogle, 'A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire', *Slate*, 11 December 2014.

North Korean Nuclear Programme (2016)

The *New York Times* reported that the US has used a variety of cyber capabilities to disrupt North Korea's nuclear missile programme.[126] Although the details are sketchy, this is useful in illustrating how cyber operations can affect kinetic capabilities directly, and offers a potent option to advance national security objectives in a targeted fashion with little effect on the civilian population. North Korea has developed a robust cyber capability, mostly geared towards raising money for the regime, although the North Korean government's alleged sponsorship of the Sony hack was apparently motivated by wounded pride rather than funding.[127]

126. David E Sanger and William J Broad, 'Trump Inherits a Secret Cyberwar Against North Korean Missiles', *New York Times*, 4 March 2017.
127. Michelle Nichols, 'North Korea Took $2 Billion in Cyber Attacks to Fund Weapons Program: U.N. Report', *Reuters*, 5 August 2019.

Conclusion

CYBER CAPABILITIES DEVELOP at lightning speed, constantly providing new opportunities for good, but also options for mischief and aggression. The current absence of a recognised menu of state responses to cyber aggression, combined with the speed of cyber operations and the random unfolding of events, increases the risk for states to stumble into war. The response framework set out in this paper provides the basis for an international discussion of cyberspace norms and expectations. Unfortunately, for the most part, states have been unwilling to disclose their cyberspace activities publicly, so there is little information to use as the basis for a response framework. The ideas presented here are, consequently, mostly a series of educated guesses about how states view cyber operations.

Because of the lack of meaningful public dialogue on state cyber operations, it is not possible to validate the proposed framework at present. Nevertheless, a few observations are suggested on the basis of available information. For one, states appear to have a higher tolerance for kinetic effects caused by cyber operations than for kinetic effects caused by traditional kinetic means.[128] This is likely because they find the angry ones and zeros of internet packets crossing the border less threatening than foreign military forces doing the same. Even pre-positioning malware that could be used at a later time to destroy critical infrastructure has not generated much of a reaction.[129]

The cyberspace-driven increase in volume and speed has not altered the basic understanding of espionage in the service of national security.[130] As such, there does not seem to be any change in the traditional view that espionage is simply a part of international relations. States may complain and will certainly try to protect sensitive information from prying eyes, but they will also continue to try to steal each other's secrets.

Finally, although nuclear weapons development programmes are considered appropriate cyber targets, nuclear command and control systems may be – and ought to be – off limits. There is (fortunately) no empirical evidence, but interference with a state's ability to launch/refrain from

128. Generalisations are always dangerous, and there are certainly differences between the views of liberal democracies and those of more authoritarian regimes. There is evidence for this conclusion, however, in the case studies here and the literature discussed earlier.
129. See, for example, the New York Dam discussion earlier in this paper.
130. The term 'national security espionage' is used to distinguish it from commercial or industrial espionage. The latter brand of espionage, typified by China's allegedly huge, ongoing theft of intellectual property from the West, is condemned by the US, the UK, Australia and New Zealand, who all consider spying for profit to be fundamentally different from spying for national security. See Diane Bartz and Jack Stubbs, 'U.S., Allies Slam China for Economic Espionage, Spies Indicted', *Reuters*, 20 December 2018.

launching their nuclear weapons, or the ability to target their nuclear weapons, are among the few cyber actions that might be considered an act of aggression meriting an armed response in self-defence.[131]

The response framework does not discuss cyber-enabled information operations. That is not because such new information operations do not present a risk. On the contrary, those operations present some of the most serious risks to consider in this context. The 2016 Democratic National Committee hack was on the surface merely a run-of-the-mill penetration of a private entity. The subsequent release of the pilfered information, timed to affect the presidential election, drove an outsized response from the US public and political leadership. Other than nuclear command and control, information operations that leverage cyber capabilities to affect political processes are the most likely category of cyber operations to lead to an escalation in tensions.[132] This important category goes mostly unaddressed in the framework because it is simply too new, and changing rather too quickly, to provide the basis for even tenuous conclusions. Modern information operations combine the ambiguity of cyberspace with the uncertainty of propaganda – and then add a dash of the 'Wild West' of social media. It is an issue that deserves analysis but is a topic beyond the scope of this paper.

As discussed throughout, there are limitations to the applicability of the model set out here. States are concerned about giving up too much by advertising cyber 'red lines' and are apprehensive about setting public standards that they might themselves not be too keen to meet. These concerns are perhaps the primary policy reasons for the reluctance of state officials to offer clear guidance. More mundane considerations are also at play. While international norms and law inform state decisions, strategic choices are ultimately driven by politics and relative power. The most any model can hope to do is provide ideas to inform states' debate about cyber engagement and national policies.

The framework presented in this paper will have served its purpose if it sparks conversation among states about avoiding cyber escalation. It would be even better if it motivates internal government consideration about articulating – and following – realistic norms of appropriate state behaviour in cyberspace.

131. For a discussion of the dangers of cyber aggression directed at nuclear command and control systems, see Jon Lindsay, 'Digital Strangelove: The Cyber Dangers of Nuclear Weapons', *Lawfare*, 12 March 2020.
132. Brown, 'Addressing Cyber-Enabled Information Operations'.

About the Author

Gary D Brown is Professor of Cyber Law at the College of Information and Cyberspace, National Defense University, Washington, DC. He has been a Cyber Policy and Strategy Analyst for the US Department of Defense Joint Staff Strategy, Plans, and Policy (J5), Cyber Policy Division, and Professor of Cyber Security at Marine Corps University, Quantico, Virginia. He served 24 years with the US Air Force, retiring as a colonel after completing his final assignment as the first senior legal counsel for US Cyber Command.