Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling

Sico van der Meer
Netherlands Institute of International Relations 'Clingendael'

Introduction[1]

Deterrence of cyber-attacks by states or state-sponsored actors is becoming an increasingly important issue in international relations. The number of cyber-attacks in the world has grown sharply in recent years; especially instances of large-scale cyber espionage and cybercrime all over the world.[2] These types of cyber aggression cause primarily economic damage. Yet, in addition to economic consequences, such as weakening the competitive economic position of a state, cyber espionage in particular is also a security issue: it can be used by enemies to learn a great deal about another nation's security situation and discover potential weaknesses. Stolen information about, for example, military capabilities or vital infrastructure, could be used to cause harm through digital or non-digital means.

Cyber-attacks aimed at sabotaging or disrupting societies are far less common so far. Nevertheless, continuing digitalization is increasing the risk of more large-scale cyber-attacks aimed at disrupting societies and creating unrest, disorder, or even causing physical damage and victims. The worldwide number of devices and appliances that are connected to each other and to the Internet will increase to approximately 25 billion in 2020.[3] The greater the dependence on cyber technologies, the more vulnerable any society will be to cyber threats. A major cyber-attack remains a possible nightmare scenario. Much damage could be caused by cyber-attackers who succeed in sabotaging energy supply systems, chemical plants, nuclear installations, air and railway traffic control systems, hospitals, drinking water and sewerage facilities, payment systems, or a combination of these. In this sense, what applies to terrorist attacks also applies to cyber-attacks: although the probability of an attack may be relatively low in statistical terms, the impact of such an attack could be considerable. From that perspective, the trend of many states heavily investing in cyber forces is not reassuring.[4]

For states, the increasing threat of large cyber-attacks is not an easy challenge. Ideally, enemies are deterred before they actually launch a cyber-attack, so no damage is done at all. To deter cyber-attackers, their cost-benefit calculation needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits. This article concisely discusses the main policy options that are relevant for deterring major cyber-attacks by other states or state actors. The options are grouped into three main categories:

1) Deterrence by Denial;
2) Deterrence by Retaliation; and
3) Deterrence by Signaling.

Deterrence by Denial

The most obvious way to deal with cyber threats is making such attacks more difficult for potential assailants by improving the security of cyber technology systems. One could label this as "defense" of a state's cyber domain, as "deterrence by denial", or as "passive deterrence" – passive because this policy is aimed at strengthening internal resilience, instead of actively influencing any actors from abroad. Deterrence by denial generally consists of technical defense measures, for example: multi-layered firewalls, advanced encryption, thorough authentication methods, so-called 'honeypots,' and active monitoring of uncommon activities in networks.

Improving the security of cyber infrastructure increases the costs that an attacker must incur to carry out a successful cyber-attack, and makes it less likely that the attack will have the desired effects and gains. If opponents know beforehand that the defense of a certain cyber infrastructure is well constructed, they will be less likely start a cyber-attack (but instead may look for other ways to attack – or attack another potential victim). To achieve this, the cyber infrastructure must be secured in such a way as to ensure that any attackers encounter barriers that considerably reduce the likelihood of their attack succeeding.

Cyber defense is regularly regarded as the best way to deal with international cyber threats.[5] An important problem, however, is that cyber defense is expensive and complex and requires continuous investment; technological developments occur at such a rapid rate in the cyber domain that any stagnation means decline. In addition, it is difficult to raise full awareness on the part of all people involved. Cyber-attackers always exploit the weakest link in the chain that they can find, and often, these weakest links are human beings. A cyber-attacker targeting a certain organization will need only one inattentive employee who downloads infected files, thereby creating an opening for the cyber-attacker.

Another problem with deterrence by denial is that cyber-attackers always have the advantage of time to look for weaknesses in cyber infrastructure, while the targeted party must respond as soon as a previously unknown weakness is exploited. In other words, cyber-attackers always have the element of surprise, making defense more complicated. Even more, because cyber-attackers immediately look for other weaknesses as soon as a gap in security has been closed, they always have an advantage over cyber defenders, especially because it is impossible to close every security gap in cyber infrastructure. Cyber defense will therefore always be a competition between attackers exploiting or seeking to exploit a newly discovered weakness, and defenders working to close a detected security gap as quickly as possible. From a deterrence perspective, cyber defense is only effective if it really changes the cost–benefit calculus of enemies. If the attackers consider it worthwhile to increase their efforts to surpass the improved cyber security measures, deterrence by denial has limited effect.

Deterrence by Retaliation

A more active method of deterrence is changing the cost-benefit calculus of potential cyber-attackers by openly communicating the possibility of retaliation and doing so if cyber-attacks are conducted. Retaliation of cyber-attacks could be done through retaliatory measures within the cyber domain itself (a cyber-attack on the attacker carried out by the party first attacked), diplomatic and/or economic sanctions, or even conventional military action. Furthermore, retaliation can be done overtly or covertly. To a certain extent, fear for retaliation will undoubtedly raise the threshold for cyber-attackers.

Economic retaliation of cyber-attacks through instituting (or strengthening pre-existing) economic sanctions might have some value as a deterrent, especially against countries with an economy that is highly dependent on trade relations with the retaliating state. However, once the sanctions are installed or strengthened, the sanctioned state has little reason to change its cyber behavior unless there are guidelines on how to ease or get rid of the sanctions. Another risk is that the economic interdependence is mutual, so economic sanctions will hurt the retaliating state as well. This is even more the case if the retaliated state will reply with counter-sanctions; in that case one could question whether the economic damage would outweigh the deterrent effect regarding cyber-attacks.

Retaliation by counter-attacks in cyberspace may be a more effective deterrent; the most obvious option to retaliate is to strike back in the same realm as the offender. The threat of counter-attacks in the cyber domain may considerably change the cost-benefit analysis of potential cyber-aggressors. On the other hand, retaliating a cyber-attack with another cyber-attack bears the risk of escalation through a tit-for-that cycle of cyber-attacks from both sides.

Another (though less realistic) option is retaliation through conventional military means, such as a strike against a specific location related to the cyber forces of the attacking state. Such an action may easily trigger a military response from the target state and could culminate in a dangerous process of escalation. This method seems likely to be considered only in the case of very destructive cyber-attacks, or if the attacker involved is considerably less powerful and will not be able to strike back militarily.

A final option of deterrence by retaliation is the use of covert military operations. It is the invisibility, and therefore unpredictability, of covert retaliation that might deter opponents from conducting cyber-attacks. Ideally, the opponent never knows whether arising cyber problems are created by covert retaliatory activities or other causes. Of course, covert retaliation also brings a risk of escalation: the target state may retaliate itself, and maybe for problems that were not caused by covert operations in the first place.

Even apart from the risk of escalation, various specific characteristics of the cyber domain make it relatively difficult to apply deterrence by retaliation effectively. The main obstacle is the attribution problem.[6] It is very difficult to conclusively identify the actor(s) responsible for unclaimed cyber-attacks. Cyber weapons differ from other weapons, as the origins of cyber weapons are not clearly visible and traceable. For example, attackers can use a chain of hacked or infected computers without the owners of these computers actually being aware of any wrongdoing. Although it is technically possible to locate the source of a cyber-attack by means of IP addresses, there is always the possibility that the source identified was merely a link in the chain of the attack and that the owner was not in any way deliberately involved in the attack.

In addition, state actors can conceal their involvement by having cyber-attacks carried out by non-state actors, like criminal hacker groups. Conversely, non-state attackers may claim an association with a given state even if this is not actually the case. It is even possible to plant "false flags" into cyber attacks, by deliberately leaving traces to another, non-involved actor (for example, by using language or computer codes linking this third actor). Because it is difficult to establish the identity of the actor responsible for a cyber-attack with absolute certainty, especially if the accused actor denies involvement, there is a risk of retaliating against an innocent party. In practice, few state actors will be willing to take this risk, something that cyber-attackers are well aware of. Strong forensic capabilities in the cyber domain are crucial to identifying the cyber-attackers; a higher probability of being identified will certainly have a deterrent effect. Currently, only very few states that have the capabilities to combine sophisticated cyber forensics with outstanding traditional intelligence operations may be able to acquire accurate, convincing evidence about cyber-attackers. Yet, openly presenting the evidence acquired may entail the risk of hurting future intelligence operations because opponents may gain insight into the intelligence capabilities that were applied.

The credibility of the retaliation threat and the risk of escalation are problems as well. Deterrence by retaliation only works if the party seeking to deter communicates clearly about the retaliatory measures that may be taken in the event of a cyber-attack. If communication about possible retaliatory measures is not clear, it is unlikely that a potential attacker will take them into account and they will therefore not have a deterrent effect. After all, deterrence measures are only effective if the opponent is aware of them. Moreover, drawing 'red lines' in the cyber domain can also have the opposite effect to potential opponents. Cyber-attackers may deliberately cross a red line to cause escalation, perhaps even while taking advantage of the attribution problem and posing as a different party. To maintain the credibility of deterrence, the party using it as an instrument must retaliate – even if doing so at that specific time is not the favored course of action. Any failure to adhere to the deterrence mechanisms communicated would dilute the deterrent effect, since potential opponents would be encouraged to think that the red lines are not all that red in practice.[7] From this perspective, deterrence by retaliation may increase the risk of a vicious cycle of escalating hostilities as well.

Deterrence by Signaling

A third category of cyber deterrence is actually a mix of deterrence by denial and deterrence by retaliation, which, on a scale of escalation risk, could be placed between the two. Deterrence by signaling is mainly about influencing the cost-benefit calculus of cyber-attackers through communication.

The foreign policy instrument of signaling consists of giving a signal to an adversary to express knowledge as well as discontent about certain behavior of this adversary. Thus, the actor in question may be convinced to stop the signaled behavior, realizing that any continuation will be noticed and potentially result in retaliation.[8] Generally, it is as simple as just communicating that the behavior of the adversary is known and deemed undesirable. This can be done in private, only known between the two adversaries, or in public, which makes the instrument more like "naming and shaming." Diplomatic protests (for example, expelling diplomats) or legal measures (for example, indicting specific persons involved with cyber aggression) are examples of mostly symbolic measures that have a signaling, and thus deterring, effect. Signaling aims to convince the adversary that continuing the activity in

> *To effectively deter cyber-attackers, their cost-benefit calculus needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits.*

question may result in countermeasures. This implies that effective signaling entails the (indirect) threat of potential retaliation as well. This way, the cost-benefit calculus behind the signaled behavior is influenced: continuing will be more costly than was (assumingly) expected before the signal was received. Yet, to support the signaling instrument, retaliation options must be on the table. Without the risk of being retaliated against, signaling efforts will less easily impress the cyber aggressor.

Although signaling is often done in private, between two influential officials or politicians, doing it in public may have even more of an effect. Public naming and shaming could have negative consequences for the adversary state's reputation, with potential repercussions in the political and economic realm. The attribution problem in the cyber domain and the risk of escalation should be mentioned here as well, but the negative effects are less direct than applying deterrence by retaliation immediately. When using the instrument of signaling, it may be less necessary to provide 100% convincing evidence as compared to retaliation.

Especially in the cyber domain, signaling may be an effective deterrent. Cyber weapons are generally considered as almost "cost free." They are often effective, while being relatively cheap to use. Moreover, because of attribution difficulties, the anonymity of the user is to some extent guaranteed. Signaling, however, could change this cost-benefit calculus. If applied successfully, signaling could remove the perceived anonymity of the cyber aggressor.[9] Signaling thus provides foreign policy makers with an extra escalation level, with only psychological effects, before the next level of actual retaliation.

Diplomacy as a long-term solution

An important notion when discussing deterrence in the cyber domain is that deterrence may be effective in the short term, but diplomacy is most promising to contribute to international cyber security and stability in the long term. While deterrence policies may almost directly have positive effects on a state's cyber security, they are expensive and bear the risk of continuing escalation. Diplomacy may not offer any "quick fixes" regarding cyber security problems, but in the long term it could offer a more secure and stable international environment in which cyber-attacks conducted or supported by state actors becomes less likely.

Confidence-building measures, for example, could enhance interstate cooperation, transparency, and predictability, with the aim to reduce the risks of misperception, escalation, and conflict entailed by cyber threats. In case of cyber aggression, confidence-building measures could function as pressure valves, allowing a safe release of tensions before they escalate. Also important are international norms and values established by multilateral diplomacy; they are to a large extent "invisible", but very influential to international security and stability. Globally-shared norms against the use of nuclear weapons, for example, contributed to the fact that their use has been nearly unthinkable for many decades. Diplomacy may contribute to establish similar norms regarding cyber-attacks. Norms can provide shared understandings between states, allowing them to consider shared interests, as well as finding ways to deal with diverging interests. Yet, the diplomatic route to establish international norms regarding cyber security is not a short-term process. To come to broadly accepted norms, common values have to be found; states must perceive that following the norms is in their own national interest.[10]

Conclusion

Deterring large cyber-attacks is not an easy task for states. To effectively deter cyber-attackers, their cost-benefit calculus needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits.

Three categories of cyber deterrence policies have been discussed above: “Deterrence by Denial” mainly means investing in cyber defense measures. It does not involve much risk for escalation, but in its passiveness it may not convince cyber-attackers to stop searching for loopholes in the cyber defenses – which will definitely be found. “Deterrence by Retaliation” is a more aggressive method: it is about ensuring cyber-attackers that they will face serious consequences when their activities are discovered. This method may have more deterrent power, but also bears serious risks of escalation and ongoing (cyber) conflict. Last, but not least, “Deterrence by Signaling” was described as a policy option. This method, which is about communicating to (potential) cyber-attackers what is known about them and what will not be tolerated, fits in between the other two options on a scale of costs, risks, and effectiveness. Ideally, a state combines all three methods in a flexible mix of cyber deterrence methods. Yet, it is also preferable that states not only focus on short-term deterrence policies, but also invest in diplomatic efforts, which may be more effective in the long term.

Sico van der Meer is a Research Fellow at the Netherlands Institute of International Relations ‘Clingendael’. His research is focusing on non-conventional weapons like Weapons of Mass Destruction and cyber weapons from a strategic policy perspective.

McNair, Washington DC. October 2016. Available at http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969675/nato-nouvelle-everything-old-is-new-again/

2 James Stavridis and Elton Parker Sailing the Cyber Sea Joint Force Quarterly #65. Fort McNair, Washington DC. April, 2012. Available at http://www.dtic.mil/docs/citations/ADA595134

3 David Aucsmith, Cyberspace is a Domain of War. May 26, 2010. Available at https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/; Martin Libicki, Cyberspace Is Not a Warfighting Domain. I/S: a Journal of Law and Policy for the Information Society. February 2012. Available at http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf

NATO Organization – Civilian Structure. Available at http://www.nato.int/cps/en/natohq/structure.htm

NATO Organization – Military Structure. Available at http://www.nato.int/cps/en/natohq/structure.htm

NATO ACT – Who We Are. Available at http://www.act.nato.int/who-we-are

When referring to NATO documents and doctrine, "defense" is spelled "defence".

All events and dates specified in this paragraph are found at NATO Cyber Defence Evolution. Available at http://www.nato.int/cps/en/natohq/topics_78170.htm#

Where NATO identifies capabilities and promotes their development and acquisition by Allies so that it can meet its security and defense objectives.

NATO Cyber Defence Pledge. Available at http://www.nato.int/cps/en/natohq/official_texts_133177.htm

Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. 6 December 2016. Available at http://www.nato.int/cps/en/natohq/official_texts_138829.htm

NATO. Cyber Defence. Available at http://www.nato.int/cps/en/natohq/topics_78170.htm

Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.

Real Clear Politics. Significant Cyberattack Incidents. Available at http://www.realclearpolitics.com/lists/cyber_attacks/intro.html

The author has identified the responsible actors based on a variety of sources

James Lewis of the Center for Strategic and International Studies publishes a comprehensive list of cyber attacks, available at https://csis-prod.s3.amazonaws.com/s3fs-public/160824_Significant_Cyber_Events_List.pdf

Allianz Global Corporate & Specialty. A Guide to Cyber Risk. September 2015. Available at http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Steve Morgan, Forbes. Jan 17 2016. Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Available at https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1b1d45b13a91

Department of Defense. Joint Publication (JP) 3-12 (R), Cyberspace Operations. 5 February 2013. Page II-4-5

Die Welt. Stoltenberg warns of spike in cyberattacks on NATO Available at http://www.dw.com/en/stoltenberg-warns-of-spike-in-cyberattacks-on-nato/a-37185594

Sky News. Fallon: NATO failing to stop Russian cyber attacks. 17 Feb 2017. Available at http://news.sky.com/story/fallon-nato-failing-to-stop-russian-cyber-attacks-10771630

NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Crossing the Cyber Rubicon. June 2016. Available at https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling

Footnotes:

[1] Parts of this article have been adapted from: Sico van der Meer, 'Defence, deterrence, and diplomacy. Foreign policy instruments to increase future cyber security', in: Cherian Samuel & Munish Sharma (eds.), S*ecuring cyberspace. International and Asian perspectives,* Pentagon Press, 2016, pp. 95-105.

[2] Virginia Harrison and Jose Pagliery, 'Nearly 1 million new malware threats released every day', CNN Money, 14 April 2015, <http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/>.

[3] International Telecommunication Union, *Trends in Telecommunication Reform 2015*, 2015, p. 4, <www.itu.int/en/publications/Documents/Trends2015-short-version_pass-e374681.pdf>.

[4] Damian Paletta, Danny Yadron, and Jennifer Valentino-Devries, 'Cyberwar Ignites a New Arms Race. Dozens of Countries Amass Cyberweapons, Reconfigure Militaries to Meet Threat', Wall Street Journal, 11 October 2015, <http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128>.

[5] David Elliot, 'Deterring Strategic Cyberattack', *IEEE Security & Privacy*, Vol. 9, 2011, No. 5, p. 38-39.

[6] Neil C. Rowe, 'The attribution of cyber warfare', in: James A. Green (ed.), *Cyber warfare. A multidisciplinary analysis*, Routledge, 2015, pp. 61-72.

[7] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Research Report, RAND Corporation, 2009, p. 65-73.

[8] Ahmer Tarar and Bahar Leventoglu, *Bargaining and Signaling in International Crises*, Research Paper prepared for the United States National Science Foundation, 2008, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.214.823&rep=rep1&type=pdf>.

[9] Sico van der Meer, *Signalling as a foreign policy instrument to deter cyber aggression by state actors*, Clingendael Policy Brief, Netherlands Institute of International Relations 'Clingendael', 2015, <www.clingendael.nl/publication/signaling-foreign-policy-instrument-deter-cyber-aggression>.

[10] Henry Farrell, *Promoting Norms for Cyberspace*, Cyber Brief, Council on Foreign Relations, 2015, <www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358>.

Toward a Global Norm against Manipulating the Integrity of Financial Data[1]

[1] This article is based on the white paper "Toward a Global Norm Against Manipulating the Integrity of Financial Data" published by the Carnegie Endowment for International Peace on March 27, 2017.

[2] G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015.

[3] G20 Finance Ministers and Central Bank Governors Meeting. G20 Communiqué. Baden-Baden, Germany, 17-18 March 2017.

[4] Krishna N. Das and Jonathan Spicer, "The SWIFT hack - How the New York Fed fumbled over the Bangladesh Bank cyber-heist," Reuters, July 21, 2016, http://www.reuters.com/investigates/special-report/cyber-heist-federal/

[5] Ibid. Section III, Para. 13(f)

[6] States' reliance on financial data and the system's interdependence is likely to increase. For example, in December 2015, The New York Times ran a story about the Swedish government's effort to move the country to an entirely cashless economy and the UN is supporting countries' efforts toward cashless economies through its Better than Cash Alliance. The Indian government is also pursuing a cashless economy.
See Liz Alderman, In Sweden, a Cash-Free Future Nears, N.Y.TIMES (April 26, 2015), http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html?_r=0;
BETTER THAN CASH ALLIANCE, https://www.betterthancash.org/ (last visited April 21, 2016).
The Indian Express, "From eradicating black money to cashless economy: PM Modi's changing narrative since demonetisation" December 22, 2016, http://indianexpress.com/article/india/demonetisation-modi-cashless-economy-black-money-narratives-4439843/

[7] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," The New York Times, August 1, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html; Richard Clarke and Robert Knake (2010) Cyber War: 202-203

[8] Russia. Draft Convention on International Information Security. 2012. Available online here: http://www.conflictstudies.org.uk/files/20120426_csrc_iisi_commentary.pdf

[9] Mark Fahey & Nicholas Wells, Charts: Who loses when the renminbi joins the IMF basekt?, CNBC (Dec. 2, 2015), http://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html; Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to be set up to check cyber frauds," India, February 1, 2017, http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854/

[10] With regard to counterfeiting currency in wartime, the general counsel of the International Monetary Fund, Francois Gianviti, wrote in a 2004 article, "Does the prohibition against counterfeit currency apply in times of war? There have been instances of such practices." For example, Germany's Operation Bernhard targeted the British economy in World War II. The U.S. government reportedly counterfeited Vietnamese and Iraqi currency during its wars with those countries. F. A. Mann, The Legal Aspect of Money, 5th ed. (Oxford: Oxford University Press, 1992); "Nazi Fake Banknote 'Part of Plan to Ruin British Economy,'" Telegraph, September 29, 2010, http://www.telegraph.co.uk/history/worldwar-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html; Lizzie Suiter, Jennifer Hucke, and Courtney Schultz, "The War at Home: A Look at Media Propaganda in WWII, Vietnam, and the War in Iraq" (final paper, Stanford EDGE program, December 2004); Youssef M. Ibrahim, "Fake-Money Flood Is Aimed at Crippling Iraq's Economy," New York Times, May 27, 1992, http://www.nytimes.