5

Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity

Sico van der Meer

Introduction

Predicting the future is hardly possible, but stating that cyber aggression – be it espionage, sabotage or even warfare – will be a continuing threat to international security and stability in the coming years seems a safe forecast. This chapter deals with the question of how states can cope with this forecast from a foreign policy perspective, focussing on cyber aggression conducted or sponsored by state actors.

Defence and deterrence, which could be labelled passive deterrence and active deterrence as well, are probably the most 'obvious' counter-measures to international cyber aggression that a state could implement. This chapter especially analyses why defence and deterrence look like promising policies, but in practice face some difficulties in the cyber realm.

Diplomatic efforts to create Confidence Building Measures (CBMs) and international accepted norms regarding cyberthreats could be more effective in actively addressing the core problems of international cyber aggression, but are little successful so far. The chapter argues that such multilateral diplomatic efforts are crucial for long-term cybersecurity and stability. Instead of an on-going 'cyber arms race', efforts could better be focussed on building mutual confidence and respect as well.

Evolving Cyberthreats

Cyberthreats, also referred to as digital threats, are generally considered as an important, and still increasing risk in international security. Cyberthreats encompass a broad spectrum. Examples include digital warfare, digital terrorism, digital espionage, digital activism and digital crime. While the purpose of each type of activity differs, in each type the weaknesses within the cyber domain are exploited to harm an 'opponent'.

It is clear that the number of cyberattacks in the world is increasing sharply over the years. It is very difficult, however, to determine the exact number of attacks, as most attacks are never reported. Indeed, individuals or organisations often remain unaware that they have been attacked, since the purpose of many cyberattacks is precisely to hack into computers or computer networks while avoiding detection.

There are so many forms and types of cybersecurity breaches, and they are committed by such a variety of actors, that it is not reasonable to analyse them as a uniform group. Cyberattacks can literally range from students who hack into other people's computers for relatively harmless fun, to large-scale industrial espionage, to digital warfare waged for the purpose of disrupting an entire society. Nevertheless, within the limitations of this chapter, a cautious attempt is made to provide a general outline of the situation, especially focussing on cybersecurity from a state-level perspective.

Especially cyberespionage and cybercrime are currently conducted at large scale, all over the world. Cyber sabotage, cyberterrorism or cyberwarfare are far less common so far. One may forecast that this frequency of the types of cyber aggression will not easily change.

The continuing digitalisation of most societies is increasing the risk of more large-scale cyberattacks aimed at disrupting society. In terms of the security of individuals and society, the greater the reliance on digitisation, the greater the impact of malicious acts carried out by parties who abuse digital environments for their own ends.

Cyberespionage and cybercrime primarily cause economic damage. In addition to economic consequences, such as weakening the competitive economic position of a state, cyberespionage in particular is also a security issue in that it can be used by potential enemies, whether state or non-state actors, to learn a great deal about the national security situation and to discover potential weaknesses. Stolen information about vital infrastructure or military capabilities, for example, could be used to cause harm by digital or non-digital means.

Whereas cyberattacks on organisations, companies and individuals are by now fairly common throughout the world, there have so far been only a few cyberattacks aimed at causing large-scale disruption in society. The most well-known examples

are the attacks that took place in Estonia in 2007 (attacks on the government, banks and media), the US (attacks on various banks) and South Korea (banks and media) in 2012. There are also examples of large-scale cyberattacks that were carried out for different purposes: Georgia in 2008 (by Russia to support its conventional military operation), Iran in 2010 (aimed at sabotaging the country's nuclear programme), Saudi Arabia in 2012 (attack on state oil company, Saudi Aramco, possibly to sabotage oil exports) and the US in 2014 (attack on Sony Pictures Entertainment, possibly to prevent the release of a movie about the North Korean leader, Kim Jong-Un). Although the economic damage was considerable in a number of these cases, large-scale cyberattacks on a country's truly vital infrastructure, such as power plants, water purification plants, or, of vital importance in a country like the Netherlands: flood protection and water management systems, have as yet not taken place. Unfortunately, it cannot be excluded at all that some states will experience such kind of cyberattacks in the (near) future.

Although alertness to cyberthreats has increased considerably in most states during recent years, technological developments in the cyber domain are occurring at such a rapid rate that cybersecurity measures must constantly be modernised to keep up in the fight against those who may have an intent of doing harm. In spite of increased awareness of risks among users of cyber technology, whether they be organisations or private individuals, such users remain a weak link in the chain in terms of countering cyberthreats. To give just one example: in a highly digitalised country like the Netherlands, a governmental assessment in 2014 estimated that approximately 35 per cent of all computer users have not installed antivirus software, even though installing such software is the first and most basic step in the context of cybersecurity.[1]

A 5-10 year Forecast

Although there is currently a lack of clarity in terms of the exact number of cyber incidents, the international threat of cyberattacks – in any way – will certainly increase in the near future, mainly because of the further digitalisation of most societies, also in vital sectors. The number of devices and appliances (medical devices, household appliances and automotive devices, to mention only a few examples) that are connected to each other and to the Internet will increase exponentially worldwide to approximately 25 billion in 2020.[2] The greater the dependence on cyber technologies, the more vulnerable any society will be to cyberthreats. Because a growing number of processes are occurring in the digital domain and a growing number of devices and appliances are connected to cyber networks, the risk of these processes, devices and appliances being manipulated by unauthorised parties is increasing correspondingly.

While in many states considerable progress is being made with respect to the security of the cyber domain in terms of, for example, increasing awareness of the risks and the technological level of security of vital cyber infrastructure, other actors are also very much on the move. Many state as well as non-state actors are investing in offensive cyberwarfare capabilities; references are regularly made in this context to a cyber arms race.[3]

Because cyberattackers immediately look for other weaknesses as soon as a gap in security has been closed, they virtually always have an advantage over cyber defenders, especially because it is impossible to close every security gap in the cyber infrastructure. Cybersecurity will therefore always be a competition between attackers who are exploiting or seeking to exploit a newly discovered weakness and defenders who work to close a detected security gap as quickly as possible.

Cybercrime and cyberespionage will continue to pose the most common threats in the future. Cybercriminals are becoming more professional and their cyberattacks are becoming more sophisticated and greater in scope. Cyberespionage carried out by states as well as private organisations (industrial espionage) will likewise increase.

In addition, a major cyberterrorist attack remains a possible nightmare scenario. A great deal of damage could be caused by cyberterrorists who succeed in sabotaging, for example, energy supply systems, hospitals, chemical plants, nuclear installations, air and railway traffic control systems, flood protection and water management systems, or payment systems. Such an attack would likely lead to social unrest. In this sense, what applies to terrorism in general also applies to cyberterrorism: although the probability of an attack may be relatively low in statistical terms, the impact of such an attack would be considerable.

Actual cyberwarfare will presumably, mostly be combined with conventional warfare. It is safe to forecast that the cyber dimension of warfare will become increasingly important; even if a state has the most powerful conventional weapon systems, if an opponent is able to influence the cyber technology behind them – think of communication and command systems – they may be of less effect on the battlefield.

It is also important to bear in mind that cyber incidents in other countries can also have consequences for any state. A disruption to the American Global Positioning System (GPS), for example, could disrupt traffic in many other countries. Equally, if a cyberterrorist caused a nuclear disaster at a nuclear power plant, any radioactive fallout could also be an issue in surrounding countries, just as a cyberattack on international bank systems could disrupt payment transactions in various countries at the same time.

Dealing with the Threat: Defence

How states could most effectively deal with international cyberthreats is a subject of ongoing discussion among researchers and policymakers. Although it is probably impossible to prevent all cybersecurity breaches, it is definitely possible to prevent many of them. Here some policy options from a foreign policy perspective will be discussed: defence, deterrence, and diplomacy.

The most obvious way to deal with cyberthreats is making such attacks more difficult for potential attackers by improving the security of cyber technology systems. One could label this as 'defence' of a state's cyber domain (although one may also label it 'passive deterrence'). One could think about technical defence measures, for example: multilayered firewalls, advanced encryption and thorough authentication methods. So-called 'honeypots' can also be used to improve security. These appear to be the kind of vulnerable areas in a system that cyberattackers are looking for, but they are in fact deliberately set traps designed to gather information about the working methods of cyberattackers. In practice, especially cybercriminals are known to avoid cyber infrastructures which are known for the use of such honeypots.[4]

Improving security increases the costs that an attacker must incur to carry out a successful cyberattack and makes it less likely that the attack will have the desired effects and gains. If cyber opponents know beforehand that the defence of a certain cyber infrastructure is well-constructed, they will less likely start a cyberattack (but instead may look for other ways to attack – or to attack another potential victim). From this perspective, defence is actually turning into passive deterrence. To achieve this, the cyber infrastructure of the potential victim must be secured in such a way as to ensure that attackers encounter barriers that considerably reduce the likelihood of their attack succeeding. Government authorities, organisations and private individuals can take a major step in such cyber defence simply by remaining very aware of the dangers of cyberattacks and ensuring that the latest security systems are always installed on their devices and networks. Networks must also continuously be monitored so that countermeasures can be taken as soon as there is any sign of an attack.

Improving cyber defence (or passive deterrence) entails fewer potential pitfalls than active deterrence or new diplomatic initiatives, as will be discussed later. This is why cyber defence is regularly regarded as the best way to deal with international cyberthreats.[5] The main problem is that cyber defence 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; cyberattackers always exploit the weakest link in the chain that they can find and often these

weakest links are human beings. In a manner of speaking, this could very well be that one inattentive employee among many other employees who downloads infected files, thereby creating an opening for the cyberattacker. As stated above, in a country like the Netherlands approximately 35 per cent of users do not even have functioning antivirus software installed on their computers. There is obviously a lot of room for improvement in terms of human awareness.

Moreover, cyberattackers always have the advantage in that they have all the time to look for weaknesses in cyber infrastructure, whereas the targeted party must respond as soon as a previously unknown weakness is exploited during a cyberattack. In other words, cyberattackers always have the element of surprise which makes defence traditionally more complicated.

Dealing with the Threat: Deterrence

Considering that defence could also be labelled passive deterrence, here the policy option of active deterrence will be discussed. Active deterrence implies deterring potential cyberattackers by the possibility of retaliation. Retaliation of cyberattacks could be done by, for example, retaliatory measures within the cyber domain itself (a cyberattack on the attacker carried out by the party first attacked), diplomatic and/or economic sanctions, or even conventional military action against the attacker. In 2014, for example, the North Atlantic Treaty Organisation (NATO) decided that a cyberattack on one of its member states would be deemed to be an attack as defined in Article 5 of the North Atlantic Treaty, thus making it possible for the alliance to take military action against cyberattackers.[6] To a certain extent, deterrence would undoubtedly raise the threshold for cyber aggressors. A cost-benefit calculation by a potential attacker will surely be influenced by potential retaliatory measures.

Because of various specific characteristics of the cyber domain, however, it is relatively difficult to apply active deterrence as an instrument against cyberattackers.

The main obstacle to the effectiveness of such deterrence measures is the attribution problem. It is very difficult to conclusively identify the actor(s) responsible for (unclaimed) cyberattacks. Cyberweapons differ from other weapons, as the origins of cyberweapons 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 cyberattack by means of Internet Protocol (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 cyberattacks carried out by non-state actors (hacker groups, for example). Conversely, non-state attackers may claim an association with a given state even if this is not actually the case. Moreover, cyberattackers can strike within a very short period of time and erase their tracks immediately after they have carried out the attack. Identifying the sources of the attack, on the other hand, is a complicated and time-consuming process. It is therefore almost impossible to take retaliatory measures during or immediately after the attack. Because it is difficult to establish the identity of the actor responsible for a cyberattack with absolute certainty, especially if the accused actor denies responsibility, there is a risk of a retaliation against an innocent party. In practice, few state actors will be willing to take this risk, something that cyberattackers are well aware of.[7]

It could be argued that indisputable and conclusive evidence is not required in some cases and that retaliatory measures can be taken if it is virtually certain that a certain state or non-state actor was involved or did not seek to stop the attackers.[8] However, leaving aside whether it is desirable to adopt this route – with the risks it entails of making false accusations – the question remains whether such an approach is actually permitted under international law. This is another area in the cyber domain where developments are still in full swing.[9]

Strong forensic capabilities in the cyber domain are crucial to identifying the party guilty of a cyberattack. A higher probability of being identified will also have a deterrent effect on potential attackers. In this regard, international cooperation, such as exchanging information about cyberweapons and cyber vulnerabilities that have been detected, is likewise essential.

In addition to the difficulty of conclusively identifying the actor responsible for a cyberattack, there are other problems associated with deterrence against such attacks as well. The credibility of deterrence and the risk of escalation are key issues. Deterrence based on the possibility of retaliation only works if the party seeking to deter communicates clearly about the retaliatory measures that may be taken in the event of a cyberattack. What acts are classified as cyberattacks that will trigger retaliation? Will retaliation take place in the cyber domain or is a conventional military strike also a possibility? 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 these measures. Moreover, drawing 'red lines' in the cyber domain can also have the opposite effect to potential opponent. Cyberattackers 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 favoured

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.[10] From this perspective, deterrence may in certain circumstances even increase the risk of a vicious circle of escalating hostilities.

Another problem with deterrence based on retaliation in the cyber domain is the proportionality of the retaliatory measures. The effects of retaliation by conventional means can usually be fairly accurately assessed. The consequences of responding to a cyberattack through the cyber domain are more difficult to control, however. This is because a retaliatory cyberattack can easily have unintended consequences precisely because everything in the cyber domain is interconnected. A cyberattack on government networks, for example, may also accidentally affect networks of hospitals, water purification plants and other providers of essential services. A retaliatory attack carried out through the cyber domain may have greater effects than intended which could make the retaliating party the black sheep of the international community instead of the initial attacker.[11] The question as to when and the extent to which retaliatory measures may be taken is another problem. In the cyber domain, it is difficult to identify the boundary between acts intended to cause economic damage or disruption and obvious acts of war. There is as yet no clarity whatsoever regarding such issues.

A final key consideration is that the diversity of actors in the cyber domain makes deterrence difficult. State actors usually have interests that would be jeopardised by retaliatory action. However, non-state actors such as hacker or terrorist groups, for example, may not actually have any interests or goods of value against which a retaliatory attack could be directed, a situation which in itself undermines the credibility of retaliation. Moreover, such non-state groups, which are capable of carrying out major cyberattacks in spite of their relatively limited resources, may not always act rationally and may not even be deterred by any kind of possible retaliation.[12]

Dealing with the Threat: Diplomacy

Diplomacy plays a role in defence and deterrence as well; think, for example, of diplomatic signalling to indicate the risk of retaliation to opponents.[13] However, diplomacy can also play an important role in increasing international cybersecurity next to defence and deterrence measures.

An important difference is that defence and deterrence are likely more effective in the short term, but diplomacy is most promising to contribute to international cybersecurity and stability in the long term. While defence and deterrence have almost direct positive effects on a state's cybersecurity, they bear the risk of

continuing escalation. Ongoing investments in defence instruments may cause a 'cyber arms race' among potential opponents, and relatively minor incidents may escalate into a dangerous 'tit-for-tat' cycle of increasing seriousness because of the retaliation efforts required for effective deterrence.[14] Diplomacy may not offer any 'quick fixes' regarding cybersecurity problems, but in the long term it could offer a more secure and stable international environment in which cyber aggression becomes less likely.

Diplomacy has proven its ability to increase international security and stability regarding various other international threats, for example, the use of Weapons of Mass Destruction. The most important contribution that diplomacy has to offer to international cybersecurity are CBMs and international norms.

CBMs could enhance interstate cooperation, transparency and predictability, with the aim to reduce the risks of misperception, escalation, and conflict entailed by cyberthreats. In case of cyber aggression, CBMs could function as pressure valves, allowing a safe release of tensions before they escalate. CBMs can be both bilateral and multilateral. Various countries have agreements with other countries regarding, for example, cooperation in case of cyber aggression. An interesting regional initiative is the set of CBMs regarding cybersecurity developed by the Organisation for Security and Co-operation in Europe (OSCE).[15]

International norms established by multilateral diplomacy 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, make their use nearly unthinkable for many decades already. Diplomacy may contribute to establish similar norms regarding aggression in the cyber domain. Norms can provide shared understandings between states, allowing them to consider shared interests as well as finding ways to deal with diverging interests. Moreover, international norms facilitate cooperation among states through shared aims and terminology.

The diplomatic route to establish international norms regarding cybersecurity 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. Currently, however, many states have quite different values regarding state behaviour in cyberspace. Especially the clashing interests on the value of an open and free Internet and definitions of cybersecurity make setting international norms a difficult task.[16]

Moreover, states cannot establish norms regarding cyber issues on their own. In most states many more significant non-state players are active as well. Such non-state actors should also be incorporated in international discussions on cybersecurity norms, for example, large e-commerce firms, activists and experts. Many of them are in favour of minimum government interference in cyberspace,

which may conflict with the aims of states. Although establishing international norms may thus be a difficult and time-consuming endeavour, in the end it will be worth the effort.

It should be noted that CBMs and international norms are not legally binding and thus their success completely relies on confidence between the states involved. Legally binding instruments, like treaties or conventions on state behaviour regarding cyber aggression, seem unrealistic to achieve in the current situation – not only because of a lack of shared views among states, but also because of the difficulties in verifying compliance to legally binding instruments regarding behaviour in cyberspace.

Conclusion

In next five to 10 years, cybersecurity will be a key topic in international politics without doubt. Because of the on-going digitalisation in the world, the threats of cyber aggression in all its forms will increase as well. To deal with the risk of cyberthreats conducted or sponsored by state actors, states have several policy options available. Three of them have been discussed above: defence, deterrence and diplomacy.

While defence and deterrence policies offer good solutions in the short term, one may question whether they are able to offer international cybersecurity and stability in the long term. Both defence and deterrence policies entail a risk of an on-going cyber arms race and a cycle of escalation between potential cyber opponents.

Diplomacy may offer less results in the short term but is more promising in the long term. CBMs and international norms, which inherently must be based on mutual trust, may not always be easy to reach but in the end they could be more effective (and cheap) than a single focus on national cyber defence and deterrence strategies. In the long term, cooperation between states to establish confidence and commonly accepted norms of behaviour in cyberspace are most promising for enduring cybersecurity and stability.

NOTES

1. National Cyber Security Centrum, "Cybersecuritybeeld Nederland: CSBN-4", 2014, p. 43, at www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-4.html [in Dutch].
2. International Telecommunication Union, "Trends in Telecommunication Reform 2015", 2015, p. 4, at www.itu.int/en/publications/Documents/Trends2015-short-version_pass-e374681.pdf.
3. Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race", *Businessweek*, July 20, 2011.
4. TNO, KPN, National Cyber Security Centre & National Police (Netherlands), "European

Cyber Security Perspectives 2015", 2015, pp. 49-51, at www.tno.nl/en/about-tno/news/2015/3/european-cyber-security-perspectives-2nd-edition/.

5. David Elliot, "Deterring Strategic Cyberattack", *IEEE Security & Privacy*, 9 (5), 2011, pp. 38-39.
6. David E. Sanger, "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack", *The New York Times*, August 31, 2014, at www.nytimes.com/2014/09/01/world/europe/nato-set-to-ratify-pledge-on-joint-defense-in-case-of-major-cyberattack.html?_r=0.
7. Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, 7 (1), 2013, p. 58; Advisory Council on International Affairs (Netherlands), "Digital Warfare", Advice No. 77, 2011, p. 13, at http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf.
8. Jason Healy, "Beyond Attribution: Seeking National Responsibility in Cyberspace", *Atlantic Council Issue Brief*, 2012, at http://www.atlanticcouncil.org/en/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace.
9. For a discussion on international law and cyberattacks, see Advisory Council on International Affairs, No. 7, pp. 19-27.
10. Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Research Report, RAND Corporation, 2009, pp. 65-73.
11. Emilio Iasiello, No. 7, pp. 59-60.
12. Clorinda Trujillo, "The Limits of Cyberspace Deterrence", *Joint Forces Quarterly*, 75 (4), 2014, p. 49; Emilio Iasiello, No. 7, pp. 64-65.
13. 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, at www.clingendael.nl/publication/signalling-foreign-policy-instrument-deter-cyber-aggression.
14. Sico van der Meer and Frans-Paul van der Putten, "US Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations", *Clingendael Policy Brief*, Netherlands Institute of International Relations 'Clingendael', 2015, at www.clingendael.nl/publication/danger-proliferating-covert-cyber-operations.
15. Organisation for Security and Co-operation in Europe, "OSCE Decision 1106", PC.DEC/1106, 2013, at http://www.osce.org/pc/109168?download=true.
16. Henry Farrell, "Promoting Norms for Cyberspace", *Cyber Brief*, Council on Foreign Relations, 2015, at www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358.