Appendix 2
Deterrence as a security concept against cyber threats

Sico van der Meer

Current situation

Cyber threats, also referred to as digital threats, are among the greatest threats currently facing the Netherlands.[1] Cyber threats 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, the use of technology is the same in all cases in that weaknesses within the cyber domain are exploited.

It is clear that the number of cyber attacks is increasing sharply. 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 attacks is precisely to hack into computers or computer networks while avoiding detection. There are so many forms and types of cyber security breaches, and they are committed by such a variety of actors, that it is not reasonable to view such breaches as constituting some kind of uniform whole. Cases 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 a society in its entirety. Nevertheless, within the limitations of this publication, a cautious attempt is made to provide a general outline of the current situation.

In its most recent cyber security assessment, the Dutch National Cyber Security Centre (NCSC) identifies cyber espionage and cybercrime as being the greatest cyber threats to the Netherlands at the present time.[2] This is especially the case because these are the two kinds of cyber attacks that, by quite a margin, occur the most frequently in the Netherlands. In addition, the NCSC observes that the continuing digitisation of Dutch society is increasing the risk of more large-scale cyber attacks 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. Cyber espionage and cybercrime primarily cause economic damage. In addition to economic consequences, such as weakening the competitive position of the Netherlands, cyber espionage in particular is also a security issue in that it can be used by potential enemies of the Netherlands, whether state or non-state actors, to learn a great deal about the national security situation in the Netherlands and discover potential weaknesses. Stolen information about vital infrastructure or military operations, for example, could be used to do damage by digital or non-digital means.

[1] General Intelligence and Security Service (AIVD), Jaarverslag 2013. The Hague: AIVD, April 2014.

[2] National Cyber Security Centre (NCSC), Cybersecuritybeeld Nederland: CSBN-4, July 2014, p. 7.

Whereas cyber attacks on organisations, companies and individuals are by now fairly common throughout the world, there have so far been only a few cyber attacks aimed at causing large-scale disruption to society. The most well-known examples are the attacks that took place in Estonia in 2007 (attacks on the government, banks and media), the United States in 2012 (attacks on various banks) and South Korea in 2012 (banks and media). There are also examples of large-scale cyber attacks 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 United States in 2014 (attack on Sony Pictures Entertainment, possibly to prevent the release of a movie about North Korean leader Kim Jong-un). Although the economic damage was considerable in a number of these cases, large-scale cyber attacks on a country's truly vital infrastructure, such as power or water purification plants, or, of vital importance in the Netherlands, flood protection and water management systems, have as yet not taken place.

Although alertness to cyber threats has increased considerably in the Netherlands in recent years, technological developments in the cyber domain are occurring at such a rapid rate that cyber security measures must constantly be modernised to keep up in the fight against those who are intent on doing harm. At present in the Netherlands, it is mainly cyber experts of specialist companies and government agencies (the National Cyber Security Centre and the Dutch Ministry of Defence's Cyber Command, for example) who are permanently engaged in battling cyber threats. 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 cyber threats. To give just one example, the NCSC notes in its most recent assessment that approximately 35 percent of all users have not installed antivirus software on their computers, even though installing such software is the first and most basic step in the context of cyber security.[3]

Expectation for the coming five to ten years

Although there is currently a lack of clarity in terms of the exact number of cyber incidents, the cyber threat to the Netherlands will certainly increase in the near future, mainly because of the further digitisation of Dutch society, also in vital sectors. The number of devices and appliances (medical devices, household appliances and automotive devices, for example) that are connected to each other and to the internet will increase exponentially worldwide to approximately 25 billion in 2020.[4] The greater this dependence, the more vulnerable society will be to cyber threats. 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.[5]

While 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

[3] National Cyber Security Centre (NCSC), Cybersecuritybeeld Nederland: CSBN-4, July 2014, p. 43.

[4] Idem, p. 77.

[5] Idem; Jan Rood, Een wankelende wereldorde: Clingendael Strategische Monitor 2014. The Hague: Clingendael, Netherlands Institute of International Relations, 2014, p. 110-119 and p. 126-128.

countries, including the Netherlands, as well as non-state actors are investing in offensive cyber warfare capabilities; references are regularly made in this context to a cyber arms race.[6] Because cyber attackers immediately look for other weaknesses as soon as a gap in security has been closed, they virtually always have the advantage. This is because it is impossible to close every security gap in cyber infrastructure. Cyber security 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 given security gap as quickly as possible.

Cybercrime and cyber espionage will continue to pose the main threats in the future, and therefore they will remain a threat to national security. Cyber criminals are becoming more professional and cyber attacks are becoming more sophisticated and greater in scope. Cyber espionage carried out by states as well as private organisations (industrial espionage) will likewise increase. It is possible that allies will in the future also engage in espionage through the cyber domain. In addition, a major cyber terrorist attack remains a possible nightmare scenario. A great deal of damage could be caused by cyber terrorists who succeed in sabotaging, for example, the energy supply, flood protection and water management systems, hospitals, chemical plants, air and railway traffic control 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 cyber terrorism: although the probability of an attack is relatively low in the Netherlands in statistical terms, the impact of such an attack would be considerable.

Actual cyber warfare directed against the Netherlands is unlikely, although a diplomatic conflict between the Netherlands and another state could perhaps also result in the disruption of certain cyber services (see the examples from abroad given above).

It is also important to bear in mind that cyber incidents in other countries can also have consequences for the Netherlands. A disruption to the American Global Positioning System (GPS), for example, could also disrupt traffic in the Netherlands. Equally, if a cyber terrorist caused a nuclear disaster at a nuclear power plant elsewhere in Europe, any radioactive fallout could also be an issue in the Netherlands, just as a cyber attack on the European Central Bank (ECB) could disrupt Dutch payment transactions. Increasing digitisation is therefore also increasing the interconnectedness between the Netherlands and other countries.

The relevance of deterrence as a security concept

Defence and deterrence capabilities against cyber threats are very much a subject of discussion among researchers and policymakers. Although it is probably impossible to prevent all cyber security breaches, deterrence may prevent some cyber attacks.

With regard to the costs side, potential attackers could be deterred by the possibility of, for example, 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 against the attacker. In 2014, for example, NATO, of which the Netherlands is a member, decided that a cyber attack on one of its member states would

[6] See for example Michael Riley and Ashlee Vance, 'Cyber Weapons: The New Arms Race'. In: Businessweek, 20 July 2011.

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 cyber attackers.[7] To a certain extent, such deterrence would undoubtedly raise the threshold. Because of various specific characteristics of the cyber domain, however, it is relatively difficult to apply deterrence as an instrument against cyber attackers.

The main obstacle to the effectiveness of such deterrence measures is the attribution problem. It is extremely difficult to conclusively establish the identity of the actor or identities of the actors responsible for an unclaimed cyber attack. Cyber weapons are not like conventional 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 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 (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, cyber attackers 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 virtually impossible to establish the identity of the party responsible for a cyber attack with absolute certainty, especially if the accused denies responsibility, there is also the risk of a retaliatory measure being taken against an innocent party. In practice, few state actors will be willing to take this risk, something that cyber attackers are aware of.[8] It could perhaps 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.[9] 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.[10]

Strong forensic capabilities in the cyber domain are crucial to identifying the party guilty of a cyber attack. 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 cyber weapons and cyber vulnerabilities that have been detected, is likewise essential.

In addition to the difficulty of conclusively identifying the party guilty of a cyber attack, there are other problems associated with deterrence against such attacks. The credibility of deterrence and the risk of escalation are key issues. Deterrence based on the possibility of

[7] David E. Sanger, 'NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack'. In: The New York Times, 31 August 2014.

[8] Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?'. In: Journal of Strategic Security. 7 (2013) 1, p. 58; Advisory Council on International Affairs (AIV), Digitale Oorlogvoering, 77 (2011), p. 13.

[9] Jason Healy, 'Beyond Attribution: Seeking National Responsibility in Cyberspace'. In: Atlantic Council Issue Brief (2012).

[10] For a discussion on international law and cyber attacks, see Advisory Council on International Affairs (AIV), Digitale Oorlogvoering, p. 19-27.

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. What acts are classified as cyber attacks 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 which actions will result in their implementation. The difficulty is that drawing 'red lines' in the cyber domain can also have the opposite effect to the one intended. 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 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.[11]

A third 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 cyber attack through the cyber domain are more difficult to control, however. This is because a retaliatory cyber attack can easily have unintended consequences precisely because everything in the cyber domain is interconnected. A cyber attack 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 the ones intended and make the retaliating party the black sheep of the international community.[12] 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 cyber attacks in spite of their relatively limited resources, may not always act rationally and may not even be deterred by any kind of possible retaliation.[13]

There are also other, more passive ways of making attacks more costly for potential attackers, not least by improving security in terms of, for example, multi-layered firewalls and advanced encryption and 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 cyber attackers are looking for, but they are in fact deliberately set traps designed to gather information about the

[11] Martin C. Libicki, 'Cyberdeterrence and Cyberwar', RAND Research Report, RAND Corporation (2009), p. 65-73.

[12] Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?' p. 59-60.

[13] Clorinda Trujillo, 'The Limits of Cyberspace Deterrence'. In: Joint Forces Quarterly, 75 (2014) 4, p. 49; Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', p. 64-65.

working methods of cyber attackers. In practice, cyber criminals avoid the Netherlands and Dutch servers because of the use of honeypots. In other words, honeypots have a deterrent effect.[14]

Improving security increases the costs that an attacker must incur to carry out a successful attack and makes it less likely that the attack will have the desired effect and secure the desired gains. To achieve this kind of deterrence, the cyber infrastructure of the potential victim must be secured in such a way as to ensure that any attackers encounter barriers that considerably reduce the likelihood of their attack succeeding. Government authorities, organisations and private individuals can take a major step towards passive deterrence simply by remaining aware of the dangers of cyber attacks and ensuring that the latest security systems are always installed on their computers and computer networks. Networks must also continuously be monitored so that countermeasures can be taken as soon as there is any sign of an attack.

Improving security, or passive deterrence, entails fewer potential pitfalls than active deterrence.[15] The main problem is that this form of deterrence is expensive and complex and requires continuous investment; technological developments occur at such a rapid rate in the cyber domain that stagnation means decline. In addition, it is difficult to raise awareness on the part of all concerned, even though a certain level of awareness is necessary, since cyber attackers always exploit the weakest link in the chain that they can find. In a manner of speaking, this could very well be that one inattentive employee who downloads infected files, thereby creating an opening for the attacker. As stated above, approximately 35 percent of users do not even have antivirus software installed on their computers. There is therefore a lot of room for improvement in terms of awareness. Moreover, cyber attackers always have the advantage in that they have all the time to look for weaknesses in cyber infrastructure, whereas the targeted individual or organisation must respond as soon as a previously unknown weakness is exploited in a cyber attack. In other words, cyber attackers always have the element of surprise.

It is important to realise that the Netherlands is not an isolated entity in the cyber domain. Regardless of the methods used to reduce cyber threats, international cooperation will always be necessary. As a method to decrease the number and danger of cyber threats, deterrence will also usually be used in the context of international alliances such as the EU and NATO. In the cyber domain, deterrence is as yet still a concept that is surrounded by many questions and problems. Nevertheless, it is in any case clear that investing in security has a certain deterrent effect. Good cyber security does not just increase the costs that an attacker must incur to carry out a successful attack, it also makes it less likely that the attack will have the desired effect and secure the desired gains.

[14] KPN (in cooperation with the Netherlands Organisation for Applied Scientific Research, the police and the National Cyber Security Centre), 'European Cyber Security Perspectives 2015', p. 49-51.

[15] David Elliot, 'Deterring Strategic Cyberattack'. In: IEEE Security & Privacy, 9 (2011), p. 38-39.