BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS 26 (2015) 193-205

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Enhancing International Cyber Security

A Key Role for Diplomacy

Sico van der Meer
Research Fellow, Netherlands Institute of International Relations Clingendael

Abstract

Cyber aggression is an increasing threat to international security and stability. While national policies intended to deter cyber aggression may offer some solution in the short term, their effects in the long term are doubtful. National cyber-deterrence policies entail the risk of an on-going cyber arms race and a cycle of escalation between potential cyber opponents. Diplomacy may offer fewer results in the short term, but it is more promising in the long term. Confidence-building measures and international norms and values may not be easy to reach, but in the end they could be more effective (and cheaper) than a single focus on national cyber-deterrence strategies. In the long term, cooperation between states to establish confidence and commonly accepted norms of behaviour in cyber space are the most promising ways available to achieve enduring cyber security and stability. Enhancing interstate co-operation, transparency and predictability of behaviour in cyberspace will reduce the risks of misperception, escalation and conflict.

Keywords

cyber security – diplomacy – defence – deterrence – norms – international relations – international conflict – international cooperation – ICT – digital infrastructure

Introduction

Cyber threats, also referred to as digital threats, are increasingly considered important risks to national and international stability and security. Cyber threats encompass a broad spectrum of illicit activities; examples include digital warfare, digital terrorism, digital espionage, digital activism and digital crime.

 | DOI 10.1163/18750230-02602004

While the purpose of each type of cyber aggression may differ, all forms of cyber aggression exploit weaknesses in the cyber domain to harm others.

In response to the perceived threat, an increasing number of states is more or less openly investing in cyber warfare capabilities, both offensive and defensive. An international trend can be observed in which states try to arm themselves in the cyber domain to deter potential cyber opponents. In this context, references are regularly made to a "cyber arms race".[1]

From a foreign-policy perspective, deterrence may indeed seem the most obvious counter-measure to international cyber threats that a state could implement. However, this article argues that deterrence looks like a promising policy but in practice encounters problems in the cyber domain and may thus be effective only in the short term. Thus, multilateral diplomatic efforts are needed to achieve long-term cyber security and stability among state actors. Diplomatic efforts to create confidence-building measures and internationally accepted norms and values regarding state behaviour in cyberspace have not been very successful so far, but on-going efforts are required because they could best address the increasing international cyber threats in the long term.

Increasing Cyber Threats

The number of cyber-attacks in the world has increased sharply in recent years. It is very difficult, however, to determine the exact number of attacks, as most are never reported. Indeed, individuals and organisations often remain unaware that they have been attacked, since the purpose of many cyber-attacks is precisely to hack into computers or computer networks while avoiding detection. Even when cyber-attacks are noticed by computer or network owners, they are often not reported out of embarrassment or fear that reporting may cause even more damage. Think of companies that do not want their customers and shareholders to get the impression that they have been sloppy with cyber security.

Moreover, 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

1 Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race", in *Businessweek*, 20 July 2011; Damian Paletta, Danny Yadron, and Jennifer Valentino-Devries, "Cyberwar Ignites a New Arms Race. Dozens of Countries Amass Cyberweapons, Reconfigure Militaries to Meet Threat", in *Wall Street Journal*, 11 October 2015, <http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128>.

to analyse them as a uniform group. Cyber-attacks range from a lone student hacking into another person's computer for relatively harmless fun to large-scale industrial espionage and to digital warfare waged for the purpose of disrupting an entire society. Nevertheless, within the limitations of this article, a cautious attempt is made to provide a general outline of the situation with a special focus on cyber security from a state-level perspective.

Cyber espionage and cybercrime in particular are currently conducted on a large scale all over the world. These types of cyber aggression primarily cause economic damage. In addition to economic consequences, such as weakening the competitive economic position of a state, cyber espionage is 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, for example, vital infrastructure or military capabilities can be used to cause harm by digital or non-digital means.

Crime and espionage will most likely continue to pose the most common cyber threats in the near future. Cyber criminals are becoming more professional, and their cyber-attacks are becoming more sophisticated and growing in scope. Cyber espionage carried out by states and private organisations (industrial espionage) will likewise increase.

Cyber sabotage or cyber terrorism are far less common so far. However, the continuing digitalization of most societies is increasing the risk of more large-scale cyber-attacks aimed at disrupting society. 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 worldwide will increase exponentially to approximately twenty-five billion in 2020.[2] The greater its dependence on cyber technologies, the more vulnerable a society is to cyber threats. Because a growing number of processes are occurring in the digital domain and an increasing number of devices and appliances are connected to cyber networks, the risk of the processes, devices and appliances being manipulated by unauthorised parties is increasing correspondingly. In terms of the security of individuals and society, the greater the reliance on digitalisation, the greater the impact of malicious acts carried out by parties who abuse digital environments for their own ends.

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, energy-supply systems, hospitals, chemical plants,

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

nuclear installations, air and railway traffic-control systems, flood protection and water-management systems, or payment systems. Such attacks would likely lead to social unrest. In this sense, what applies to terrorism in general also applies to cyber terrorism: although the probability of attacks may be relatively low in statistical terms, the impact of such attacks would be considerable.

Presumably, actual cyber warfare will usually be combined with conventional warfare. It is safe to predict that the cyber dimension of warfare will become increasingly important. Even the most powerful conventional-weapon systems may be debilitated by an opponent who can influence the cyber technology behind them (e.g., communication and command systems).

Whereas cyber-attacks on organisations, companies and individuals are by now quite common throughout the world, there have so far been only a few cyber-attacks aimed at causing large-scale disruption to society. The best 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: the cyber-attack in Georgia in 2008 (by Russia, to support its conventional military operation), in Iran in 2010 (aimed at sabotaging the country's nuclear programme), in Saudi Arabia in 2012 (attack on the state oil company, Saudi Aramco, possibly to sabotage oil exports), in the United States in 2014 (attack on Sony Pictures Entertainment, possibly to prevent the release of a movie about the North-Korean leader, Kim Jong-Un), and in Ukraine in 2015 (cyber-attack on a power grid, possibly by Russia-supported rebels). Although the economic damage was considerable in some of these cases, no cyber-attacks are yet known to have killed or wounded people. Nevertheless, the possibility cannot be excluded that such cyber-attacks will occur in the near future.

While discussing the threat of international cyber aggression, it is important to bear in mind that cyber incidents in any country can also have consequences for other states. A disruption to the American Global-Positioning System (GPS), for example, could disrupt traffic in many other countries. Equally, if a cyber terrorist caused a nuclear disaster at a nuclear-power plant, any radioactive fallout could also be an issue in surrounding countries. A cyber-attack on international bank systems could disrupt payment transactions in various countries at the same time.

Passive Deterrence: Cyber Defence

The most obvious way to deal with cyber threats is to make such attacks more difficult for potential attackers by improving the security of cyber-technology

systems. One could label this a "defence" of a state's cyber domain or a "passive deterrence"—passive because this policy is aimed to strengthen internal resilience instead of actively influencing any actors from abroad. Passive cyber deterrence often consists of technical defence measures: e.g., multi-layered 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 that cyber-attackers look for in a system, but they are in fact deliberately set traps that are designed to gather information about the working methods of cyber-attackers. In practice, especially cyber criminals are known to avoid cyber infrastructures that are known to use such honeypots.[3]

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. If cyber opponents know beforehand that the defence of a certain cyber infrastructure is well-constructed, they will be less likely to start a cyber-attack. (They may instead may look for other ways to attack or attack another potential victim.) To achieve this, 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 success.

It will always be necessary to invest in cyber security. In the short term, improved cyber defence (or passive deterrence) may also entail fewer potential pitfalls than active deterrence or diplomatic efforts, as discussed below. This is why cyber defence is regularly regarded as the best way to deal with international cyber threats.[4] An important problem, however, 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; cyber-attackers always exploit the weakest link in the chain, and these weakest links are often human beings. A cyber-attacker targeting a certain organization needs only one inattentive employee who downloads infected files, thereby creating an opening for the cyber-attacker. To give just one example: in a highly digitalized country like The Netherlands, a governmental assessment in 2014 estimated that approximately thirty-five percent 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 cyber

3 TNO, KPN, National Cyber Security Centre & National Police (Netherlands), "European Cyber Security Perspectives 2015", 2015, pp. 49–51, <www.tno.nl/en/about-tno/news/2015/3/european-cyber-security-perspectives-2nd-edition/>.

4 David Elliot, "Deterring Strategic Cyberattack", in *IEEE Security & Privacy*, vol. 9, 2011, no. 5, pp. 38–39.

security.[5] In general, there is often much room for cyber-defence improvement in terms of human awareness.

Another problem with passive deterrence in the cyber realm is that cyber-attackers have the advantage that they constantly look for weaknesses in cyber infrastructure while the targeted party must respond as soon as a previously unknown weakness is exploited during a cyber-attack. In other words, cyber-attackers always have the element of surprise, which makes defence traditionally more complicated. Furthermore, because cyber-attackers 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 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 detected security gap as quickly as possible.

Active Deterrence: Retaliation

In addition to passive deterrence, more and more states are opting for active deterrence of cyber aggression by other states. Active deterrence implies deterring potential cyber-attackers by raising the possibility of retaliation. Retaliation of cyber-attacks could be done, for example, by 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, the North Atlantic Treaty Organisation (NATO) decided that a cyber-attack on one of its member states would be deemed an attack as defined in Article 5 of the North Atlantic Treaty, thus making it possible for the alliance to take joint military action against cyber-attackers.[6]

To a certain extent, deterrence will 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 cyber-attackers.

---

5 Nationaal Cyber Security Centrum, "Cybersecuritybeeld Nederland: CSBN-4", 2014, p. 43, [in Dutch] <www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-4.html>.

6 David E. Sanger, "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack", *New York Times*, 31 August 2014, <www.nytimes.com/2014/09/01/world/europe/nato-set-to-ratify-pledge-on-joint-defense-in-case-of-major-cyberattack.html?_r=0>.

The main obstacle to the effectiveness of such deterrence policies is the attribution problem. 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 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 a false association with a given state. Moreover, cyber-attackers can strike within a very short period of time and erase their tracks immediately afterward. Identifying the sources of an 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 an attack. 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 responsibility, there is a risk of retaliating against an innocent party. In practice, few state actors are willing to take this risk—something that cyber-attackers are well aware of.[7]

It can 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]

7 Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", in *Journal of Strategic Security*, vol. 7, 2013, no. 1, p. 58; Advisory Council on International Affairs (Netherlands), "Digital Warfare", in *Advice*, 2011, no. 77, p. 13, <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, <http://www.atlanticcouncil.org/en/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace>.

9 For a discussion on international law and cyber-attacks, see Advisory Council on International Affairs (Netherlands), "Digital Warfare", Advice, 2011, no. 77, pp. 19–27, <http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>.

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. Currently, only the very few states that can combine very sophisticated cyber forensics with outstanding traditional intelligence operations are able to acquire accurate, convincing evidence about the perpetrators of cyber aggression. However, openly presenting the evidence acquired may hurt future intelligence operations, because opponents may gain insights into the intelligence capabilities that were applied.

In addition to the difficulty of conclusively identifying the perpetrator of a cyber-attack, there are other problems associated with deterrence by retaliation against such attacks. The credibility of deterrence and the risk of escalation are key issues. Deterrence based on the possibility of retaliation works only 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 possible? If communication about possible retaliatory measures is not clear, it is unlikely that a potential attacker will take them into account and they therefore will not have a deterrent effect. After all, deterrence measures are effective only if the opponent is aware of them. Moreover, drawing "red lines" in the cyber domain can also have the opposite effect on 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 favoured course of action. Any failure to adhere to the deterrence mechanisms communicated will dilute their effect, as potential opponents will thereby be encouraged to think that red lines are not so red in practice.[10] From this perspective, deterrence by retaliation may in certain circumstances even increase the risk of a vicious circle of escalating hostilities.

Another problem with active deterrence 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,

10 Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Research Report, RAND Corporation, 2009, pp. 65–73.

however. 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 or other providers of essential services. A retaliatory attack carried out through the cyber domain may thus 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 to what extent 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 acts of war. There is as yet no clarity whatsoever regarding such issues.

Though this article focuses on state actors, it is also important to note that the diversity of actors in the cyber domain makes active deterrence difficult. State actors usually have interests that can be jeopardised by retaliatory action. Non-state actors such as hackers or terrorist groups, however, may not actually have any interests or goods of value against which a retaliatory attack can be directed—a situation that 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.[12]

Diplomacy as a Long-Term Solution

Diplomacy is often part of deterrence policies; think, for example, of diplomatic signalling to indicate the risk of retaliation to opponents.[13] However, diplomacy can also play a key role in increasing international cyber security alongside deterrence measures. It is important to note that deterrence may be more effective in the short term but that diplomacy is the most promising way to contribute to international cyber security and stability in the long term. While deterrence measures—both passive and active—can have positive effects on

11 Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", pp. 59–60.

12 Clorinda Trujillo, "The Limits of Cyberspace Deterrence", in *Joint Forces Quarterly*, vol. 75, 2014, no. 4, p. 49; Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?", 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, <www.clingendael.nl/publication/signalling-foreign-policy-instrument-deter-cyber-aggression>.

a state's cyber security almost directly, they are expensive and bear the risk of continuing escalation. Ongoing investment in cyber security 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 cyber-security problems. In the long term, however, it could offer a more secure and stable international environment in which cyber aggression conducted or supported by state actors 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 contributions that diplomacy has to offer to international cyber security are confidence-building measures (CBMs) and international norms and values.

Confidence-building measures can enhance interstate co-operation, transparency and predictability, with the aim of reducing the risks of misperception, escalation and conflict entailed by cyber threats. In case of cyber aggression, confidence-building measures can function as pressure valves that allow a safe release of tensions before they escalate. Confidence-building measures can be taken both bilaterally and multilaterally. Various countries already have agreements with other countries regarding, for example, cooperation in case of cyber aggression.

International norms and values established by multilateral diplomacy are to a large extent "invisible", but they are very influential with respect to international security and stability. Globally shared norms against the use of nuclear weapons, for example, have contributed to the fact that their use has been nearly unthinkable for many decades already. Diplomacy may help establish similar norms regarding aggression in the cyber domain. Norms can provide shared understanding between states, allowing them to consider shared interests and to find ways to deal with diverging interests. Moreover, international norms facilitate cooperation among states through shared aims and terminology.

The diplomatic route to the establishment of 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. Currently, however, many states have

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, <www.clingendael.nl/publication/danger-proliferating-covert-cyber-operations>.

quite different values regarding state behaviour in cyberspace. In particular, clashing views about the definition of cyber security and the value of an open and free Internet make the setting of international norms a difficult task.[15]

Moreover, states cannot establish norms regarding cyber issues at their own. In most states, many more significant non-state players are also active. Such non-state actors—for example, large e-commerce firms, activists and experts—should also be incorporated in international discussions on cybersecurity norms. Many of them are in favour of minimum government interference in cyberspace, which may conflict with the aims of states. Although establishing international norms and values may thus be a difficult and time-consuming endeavour, in the end it will be worth the effort.

It should be noted that confidence-building measures and international norms are generally not legally binding. Their success therefore relies completely on confidence between the states involved. Legally binding instruments—such as treaties or conventions on state behaviour in cyberspace—seem unrealistic in the current situation, not only because of a lack of shared views among states, but also because of the difficulties in verifying compliance.

The current speed of diplomatic processes aimed to enhance global cyber security and stability is quite low, especially compared to the high speed of technological developments in the cyber domain. Yet, various noteworthy developments are taking shape. On the global level, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) should be mentioned. This group is working on proposals regarding norms of responsible state behaviour in cyberspace and on questions about how existing international law applies to this domain. The UNGGE has been working on these issues for some years already and will likely not be finished in the short term. Still, the various steps in this process are important because they may be helpful in setting internationally shared norms and values regarding state behaviour in the cyber domain.[16] The International Telecommunication Union (ITU) is also working on shared language, standards and norms.[17] Other

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

16 United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 22 July 2015, <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.

17 "ITU National Cybersecurity Strategy Guide", September 2011, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>.

regional diplomatic initiatives are producing important results as well. The set of confidence-building measures regarding cyber security developed by the Organization for Security and Co-operation in Europe (OSCE) is widely regarded as an important result of multilateral norms-building efforts.[18] The same applies to some extent to the Tallinn Manual on the International Law Applicable to Cyber Warfare, which was developed within the context of the North Atlantic Treaty Organization (NATO).[19] This initiative has been positively received by various states, including both NATO members and non-members.

Although multilateral diplomatic answers to international cyber threats are developed more slowly than unilateral cyber-deterrence policies can be implemented, they are more promising in creating enduring international cyber security and stability in the longer term. Shared values and norms are not easily set; but once they have emerged, they are powerful instruments for enhancing international security and stability. Though their current progress comes only gradually, the fact that diplomatic efforts are gaining ground is certainly a positive development.

Conclusion

It is hardly possible to predict the future, but it seems safe to say that cyber aggression will continue to be a threat to international security and stability in the coming years. While national deterrence policies may offer some solution in the short term, their effects in the long term are doubtful. National cyber-deterrence policies entail the risk of an on-going cyber arms race and a cycle of escalation between potential cyber opponents.

Diplomacy may offer fewer results in the short term, but it is more promising in the long term. Because confidence-building measures and international norms and values are necessarily based on mutual trust, they are not easy to produce. In the end, however, they could be more effective (and cheaper) than a single focus on national cyber-deterrence strategies. In the long term, cooperation between states to establish confidence and commonly accepted norms of behaviour in cyber space constitute the most promising route to enduring cyber security and stability. Enhancing interstate co-operation, transparency

18 Organization for Security and Co-operation in Europe, "OSCE Decision 1106", PC.DEC/1106 (2013), <http://www.osce.org/pc/109168?download=true>.

19 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, freely available here: <https://ccdcoe.org/research.html>.

and predictability of behaviour in cyberspace will reduce the risks of misperception, escalation and conflict. Current initiatives like the UNGGE, the OSCE set of confidence-building measures and the Tallinn Manual are important first steps towards this end.

Though it will always be necessary to invest in the security of cyber infrastructure—which may also function as passive deterrence—national restraints on investments in offensive cyber capabilities are desirable. Moreover, increased diplomatic efforts are required to accelerate the multilateral search for a long-term solution to international cyber threats.