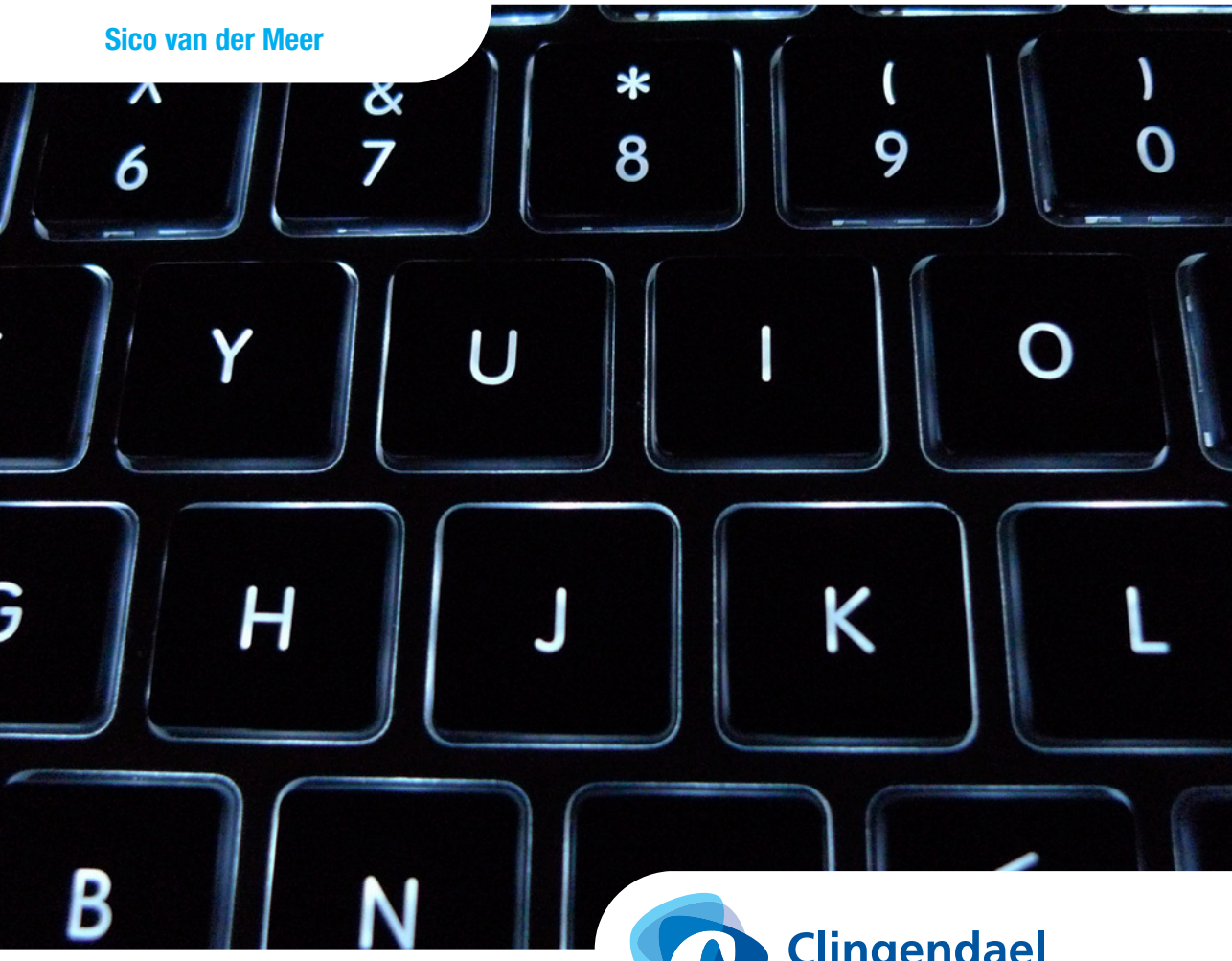
Cybersecurity

Thematic Study Clingendael Strategic Monitor 2017

Sico van der Meer



Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Cybersecurity

Thematic Study Clingendael Strategic Monitor 2017

Sico van der Meer

February 2017

February 2017

About the Author

Sico van der Meer is affiliated to the Clingendael Institute as a Research Fellow. His research focuses in particular on cybersecurity and weapons of mass destruction.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media:
@clingendael83
The Clingendael Institute
The Clingendael Institute

Email: info@clingendael.nl
Website: www.clingendael.nl

Contents

Introduction

This contribution attempts to make estimates in the field of cybersecurity for 2021. Although forecasting has always been a challenge, that applies even more to cybersecurity than to the other contributions. Cybersecurity experts regularly joke that there are two types of organisations: organisations that have been hacked and organisations that don't yet realise they have been hacked. In other words, good, reliable information is often difficult to find. This thematic study nevertheless attempts to make a number of estimates on the basis of observed trends. The contribution opens with a threat assessment and then works towards an analysis of international cooperation in the cyber domain. The conclusion is that digital threats are set to increase rapidly, while international cooperation in the field is still in its infancy. At the same time, improvements are expected in the area of international cooperation by 2021.

Threat assessment

Introduction

The European Union (EU) launched its Cybersecurity Strategy in 2013 following an alarming increase in the number of cybersecurity incidents. The EU has expressed its intention to make the European digital environment one of the safest in the world, but then without sacrificing the open and free character of the internet supported by the EU – security measures may not compromise privacy and the right to free speech.[1] The EU Global Strategy that was published in 2016 once again endorses this dual goal.[2] In the Netherlands, the first National Cyber Security Strategy was published in 2011, followed in 2013 by a second updated version. This strategy also includes a safe internet in close conjunction with economic and social benefits as well as with privacy and freedom of speech.[3]

The base rate

The digital threats facing the EU and its member states are diverse by nature. The EU faces violations that can vary from digital warfare and terrorism to sabotage, espionage, and crime. These threats are expected to increase even more in the next five years (see Table 1).

1 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, February 2013, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

2 European Commission, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, June 2016, https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf.

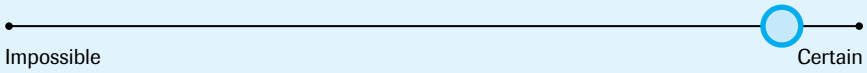
3 National Coordinator Counterterrorism and Security, *National Cyber Security Strategy 2*, 2013, https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2.

Table 1 Cybersecurity threat assessment

Trend table	Cybersecurity	Trend
Base rates	Number of businesses hacked	▲
	Cyber manipulation	▲
	Number of cyberattacks	▲
Factors	Connectivity to the Internet	▲
	Escalation potential	▲
	Cyber arms race	▲

Impact on European security interests in 2016 and 2021

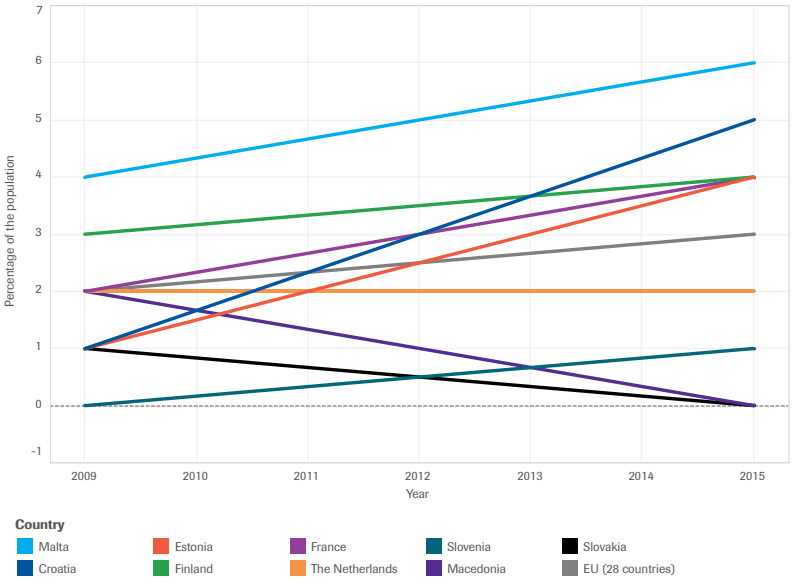
Probability of the threat's occurrence in 2021



Actors responsible for the threat

Thus far, particularly cyber espionage and cybercrime have been very common. To cite just one example: in 2015 an average of one in ten UK citizens was a victim of some type of cybercrime, making it numerically by far the largest crime category.[4] Eurostat also investigated the number of individuals in European member states that were victims of internet fraud over the past few years. Those figures are lower, but the numbers are generally showing a steady upward trend (see Figure 1). As yet, there have been relatively few concrete cases of cyber war, cyber sabotage and cyber terrorism. It is important to note, however, that there are unfortunately still no clear overviews of the numbers and types of digital attacks that are taking place. This is also partly because victims often do not even realise that their digital infrastructure has been penetrated, or they prefer to say nothing about it in order to protect their reputation or avoid insurance claims. A number of cybersecurity companies regularly publish statistics about digital security violations they have detected, but there has never been an overall picture available; Figure 2 shows how much the statistics vary. The only conclusion that can be drawn from the fragmented information is that cyber attacks of all types are increasing steadily.

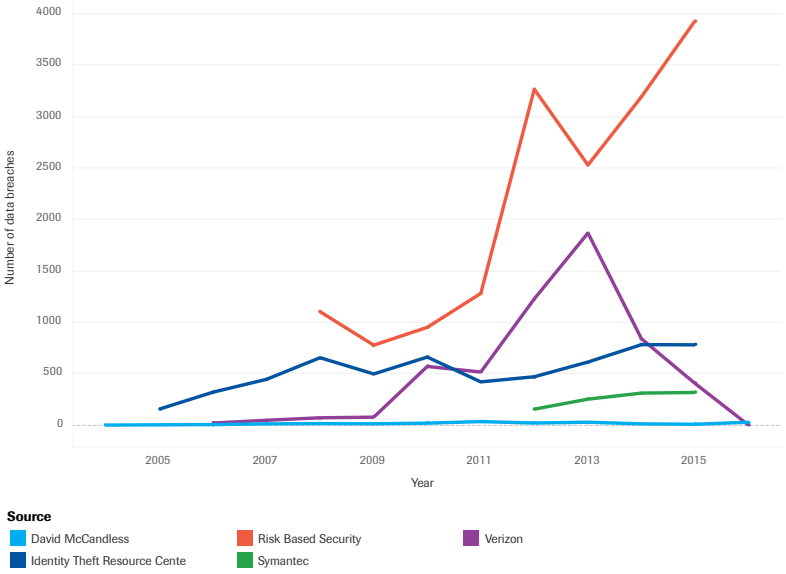
Figure 1 Percentage of individuals affected by internet fraud[5]



4 Travis, A. 2016. 'Cybercrime figures prompt police call for awareness campaign', *The Guardian*, 21 July, https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures.

5 Top 5 highest and lowest displayed – black line is EU average; Eurostat, 2009-2015, http://ec.europa.eu/eurostat/data/database.

Figure 2 Digital security violations[6]



Cyber manipulation in the political arena has also been increasing in recent years. This involves the almost unnoticed manipulation of political dynamics and public opinion, such as suspicions – which are difficult to prove – that Russia used 'information operations' to try to influence the United States (US) presidential election.[7] These types of operations, often intended to cause unrest or undermine the legitimacy of the (democratic) political processes, are expected to significantly increase worldwide – in that sense, the cyber domain is beginning to become a fully-fledged extra dimension of the international political and military sphere of activity.

Up to this point, there have been very few cases of major cyber attacks in the sense of cyber war. However, the few examples that do exist demonstrate the potential

6 Collation of David McCandless' data, 2004-2016, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; Verizon, *VCDB Database*, 2006-2016, http://vcdb.org/index.html; Risk Based Security, *Annual Reports*, 2008-2015, https://www.riskbasedsecurity.com/researchadv/; Identity Theft Resource Centre, *Annual Report*, 2005-2015, http://www.idtheftcenter.org/About-ITRC/itrc-corporate-overview.html; Symantec, *Annual Reports*, 2012-2015, https://www.symantec.com/security-center/threat-report.

7 Baraniuk, C. 2016. 'Is Russia hacking the US election?', *BBC News*, 18 August, http://www.bbc.com/news/technology-37117414; Parlapiano, A. 2016. 'What we know about the cyberattack on Democratic politicians', *New York Times*, 16 August, http://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html?_r=0.

power of such attacks. One illustration is the cyber attack on Ukraine's electricity network in December 2015, which meant that some of the population was left without energy in freezing temperatures. Earlier large-scale cyber attacks, such as the attack on government and media targets in Estonia in 2007 and the attack to support the Russian military assault on Georgia in 2008, seem almost old-fashioned compared to the technical capabilities currently observed in cyber operations with malicious intent. It is true that there have been as yet no cyber attacks resulting in deaths and injuries, but the fact that such attacks can cause physical damage has already been demonstrated in practice. Examples include the sabotage of industrial equipment in Iran (uranium enrichment plants) and Germany (steel factory), but also, for example, Saudi state oil company Saudi Aramco that had to replace thousands of its computers. Doomsday scenarios in which cyber attackers can disrupt an entire society by disabling energy, transport and communication systems for long periods have not yet actually materialised. Moreover, catastrophic scenarios in which cyberterrorists manage to launch nuclear weapons or cause aviation disasters by manipulating air traffic control systems are not impossible, but are also not very likely. Unlike the average laptop, these types of systems are actually extremely well protected.

Determining factors

Based on a number of qualitative trend-based indicators related to digital espionage, crime and war, cyber threats are expected to increase by 2021. At the same time, it is also important to look at a number of factors and examine whether the base rate needs to be adjusted further. Important indicators in this area, such as the degree of digital connectivity, the escalation potential and the extent of the cyber arms race, show that both the probability and the impact of cyber attacks require an upward rather than a downward adjustment.

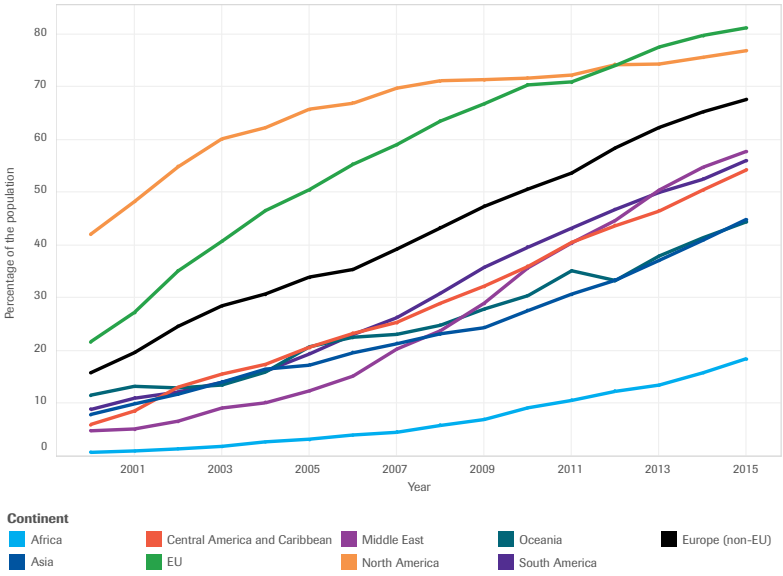
One of the main factors that can contribute to an increase in cyber attacks in the future is the growing number of internet users and the increasing prevalence of digital connectivity (see Figure 3). Modern society is becoming more and more dependent on digitisation. Not only has the number of internet users been increasing for years,[8] – the numbers of appliances and devices connected to the internet has also been growing rapidly worldwide: the International Telecommunication Union (ITU) has estimated that by the end of 2015 there were around 2.9 billion objects connected to the internet, and this number will increase to around 25 billion in 2020.[9] The concept of 'the Internet of Things' is very revealing in that sense: who would have thought five years ago that so many everyday objects such as refrigerators, thermostats and cars would be connected

8 For up-to-date statistics, see: *Internet Live Stats,* http://www.internetlivestats.com/internet-users/.

9 International Telecommunication Union (ITU), *Trends in telecommunication reform 2015*, 2015, 4, http://www.itu.int/en/publications/Documents/Trends2015-short-version_pass-e374681.pdf.

to the internet? It is incredible that even barbecues can be hacked nowadays, and they are probably the least damaging of all appliances. For criminals, spies, terrorists and the military, the abundance of vulnerabilities in the digital domain is a goldmine. The ever growing dependency on digital services in (Western) society is therefore also helping to increase the associated risks.

Figure 3 Population percentage with internet access[10]



A second factor that can contribute to the growing risk is the escalation potential – that is, possible unintended effects of cyber operations. For example, computer codes used by attackers can take on a life of their own, as is the case with an infectious virus. In this way, even small-scale cyber activities can accidentally have global consequences. And then there is the danger of rapid escalation. It is theoretically possible – but it has not yet happened openly – for a country to intentionally or unintentionally become the victim of a large-scale cyber incident and then initiate a retaliatory strike. This can trigger a spiral of escalation, while the attribution problem and 'false flag' operations (when an attacker leaves fake clues behind that incriminate another party) can cause innocent countries to be dragged into the spiral of escalation. There is also an indirect threat, as illustrated

10 ITU, *Internet Access,* 2000-2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

by a detected (trial) attempt to attack an American dam; such cyber operations are just preparatory to launching a malicious strike at a later moment.[11]

A third factor is that a global cyber arms race has been ignited, in which many countries are investing in capacities for defensive and offensive cyber war.[12] This also increases the risk of these capacities actually being deployed (whether or not due to misunderstandings, miscommunication, etc.). It is also far from reassuring that cybersecurity experts believe there are indications that state actors are preparing to cripple (parts of) the global internet.[13]

Impact and shocks

As shown by the above analysis, digital threats are increasing all the time and the nature of the threats continues to be very diverse. Digital espionage and crime in particular are causing the most of problems at the moment, mainly with economic damage as a consequence. The exact damage caused by digital attacks is unknown, however. To illustrate: in 2013 an American think tank estimated that the world economy suffers more than 400 billion dollars worth of damage annually from cybercrime and cyber espionage.[14] However, this estimate only focused on direct damage: the authors of the report stated that long-term consequences such as slower innovation, disrupted trade, increasing unemployment and diminishing confidence in the economy, government and other people are difficult to express in financial terms.

Physical damage (including physical casualties) cannot be ruled out in the not too distant future. Political and military information or data about vulnerabilities in security can end up in the possession of attackers.[15] The risk that (parts of) the population ultimately grows/grow to mistrust digital technologies is not imaginary, and can lead to social unrest and resistance to further digitisation of public services, for example. Lastly, it is noticeable that in addition to economic and physical threats, political and social threats are also on the rise. The cyber domain can be used to manipulate information

11 Kutner, M. 2016. 'Alleged dam hacking raises fears of cyber threats to infrastructure', *Newsweek*, 30 March, http://europe.newsweek.com/cyber-attack-rye-dam-iran-441940?rm=eu.

12 Paletta, D., et al. 2015. 'Cyberwar Ignites a New Arms Race', *The Wall Street Journal*, 11 October, http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.

13 Schneier, B. 2016. 'Someone Is Learning How to Take Down the Internet', *Lawfare Blog*, 13 September, https://www.lawfareblog.com/someone-learning-how-take-down-internet.

14 Center for Strategic and International Studies & Intel Security-McAfee, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

15 National Cyber Security Centre, *Cyber security situation in the Netherlands – CSBN 2016*, https://www.rijksoverheid.nl/documenten/rapporten/2016/09/05/cybersecuritybeeld-nederland-csbn-2016.

that can then affect political processes: this might include the abovementioned accusations that Russia tried to interfere in the US presidential election. Besides influencing other countries, many countries are attempting to do the same to their own population by means of internet censorship and digital propaganda.

The above projections are based on trends that are difficult to pinpoint, so they are very susceptible to all kinds of uncertainties and sudden events. To map out these projections, the Clingendael Expert Survey has identified a number of possible events and graded them (see Figure A in the Appendix). In the area of cybersecurity, they identified a large-scale Russian cyber attack as a potential shock. Suppose a conflict developed between Russia and the West (read: the North-Atlantic Treaty Organisation (NATO), or the EU); Russia could launch a massive cyber attack that inflicts major damage in the NATO and/or EU member states being attacked. This not only includes civil (social and economic) damage: a major cyber attack could also affect military capabilities – for example, by sabotaging communication and command structures in addition to energy and logistical networks. Such a large-scale cyber attack has never been launched, but it may be assumed that Russia has been involved in similar attacks on a smaller scale. Such a shock could have a major impact on international relations and the position of Europe and/or the West therein.

Cybersecurity regime

The threat assessment gives cause for concern: the number of attacks is expected to increase on almost all levels and the consequences will be more significant than is now the case. The next question is: to which extent is there an (evolving) international system of cooperation and/or harmonisation that could mitigate any possible consequences? This analysis therefore draws up a number of qualitative indicators (see Appendix 2) and successively deals with the important actors and institutions, norms and rules and the extent to which actors are in compliance with this (existing) set of (implicit) norms and rules.

Actors and institutions

One specific problem with cyber threats is the lack of international regulation: cybersecurity is often called the 'Wild West' of international relations. There are no specific international institutions in this field. Due to political divisions, the only international governmental organisation that is active in this area, the ITU, has thus far not achieved any concrete results. The United Nations (UN) only has a Group of Governmental Experts working on this theme, which is indeed very active, but has quite a lowly position in the UN bureaucracy.

However, a large number of regional and bilateral initiatives have been taken. For example, the Organisation for Security and Cooperation in Europe (OSCE) and the Shanghai Cooperation Organisation (SCO) have agreed to voluntary codes of behaviour, but they are completely non-binding. Also in the context of NATO, a cyber attack on a member state is now regarded as a cyber attack on the alliance, even though it has (consciously) not been precisely defined what is meant by a cyber attack and what exactly the reaction will be.[16] A number of countries have entered into bilateral agreements, but these agreements are often purely symbolic and focus, for example, on mutual assistance in the case of cyber attacks. In 2015, the US and China agreed to not (or no longer) spy on each other for economic reasons, after intense pressure from the US due to frustration about the extent to which China was doing this. Following the agreement, the number of cases of (assumed) cyber espionage in the US did indeed

16 Limnéll, J. and Salonius-Pasternak, C. 2016. 'Challenge for NATO: Cyber Article 5', *Center for Asymmetric Threat Studies*, Briefing Paper, June, https://www.fhs.se/documents/Externwebben/forskning/centrumbildningar/CATS/publikationer/2016/Challenge%20for%20NATO%20%E2%80%93%20Cyber%20Article%205_Brief.pdf.

diminish somewhat, even though some experts believe that this is mainly because Chinese (state) hackers began operating more clandestinely.[17]

Where the above initiatives point to a major role for state actors, one of the specific characteristics of the cyber domain is the variety of actors; states are certainly not the only significant players. For example, the physical side of the cyber domain, the infrastructure, is largely in the hands of private organisations. To cite a few examples: the data communication cables, the server nodes, and even the organisation that allocates internet addresses are usually in private hands. To achieve effective international regulations in the digital domain, it is therefore necessary to involve the many private stakeholders. However, bringing all the interested parties together in an efficient way is an enormous challenge.

Norms and rules

For now, with regard to the cyber domain, norms are being debated and there is a lack of international regulation. No specific international treaties have been signed. However, the abovementioned UN working party has stressed that the prevailing international law also applies to the digital domain.[18] How this must be translated in practice remains a problem, particularly owing to specific difficulties such as the attribution problem with cyber attacks: it is extremely difficult to provide irrefutable proof that a particular party is responsible for cyber incidents.[19]

In fact, there are as yet no international norms and rules in the cyber domain, at least no more than the generally accepted idea that international law also applies. It is unlikely that there will be greater consensus in the years to come. However, a number of initiatives were recently launched by the private sector. Microsoft is an important pioneer that proposed six international norms in 2014,[20] and in 2016 suggested setting up an international independent cyber attack attribution organisation. In this context, the private sector would be able to supply states with expertise to prevent mistaken

17 Harold, S.W. 2016. 'The U.S.-China Cyber Agreement: A Good First Step', *RAND Blog*, 1 June, http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.

18 Report issued by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, Document A/70/174, July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

19 Healy, J. 2012. 'Beyond attribution. Seeking national responsibility for cyber attacks', *Atlantic Council,* Issue Brief, http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

20 McKay, A., et al. 2014. 'International Cybersecurity Norms: Reducing conflict in an Internet-dependent world', *Microsoft*, http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

attribution and hasty reactions from causing major problems.[21] Although these types of private initiatives have been broadly acclaimed, they have not yet led to concrete results. However, the fact that large companies deem it desirable to stimulate national governments to take measures to increase worldwide digital security is a development that will probably be followed up, given the major interests of multinationals in this area.

Important contentious issues that are standing in the way of international state cooperation include the differing opinions of states about the nature of the cyber domain and the role of the state in this area. There is a group of states (particularly the major powers of China and Russia) that want to increase state control of the internet from the perspective of national security. On the other hand, another group of states (with the US and the EU as the main representatives) regard the internet as a public domain in which freedom and the open geographical borders are the priority. Government agencies must interfere as little as possible in this area, even if some of the states that support a free internet are guilty of digital espionage.

Compliance

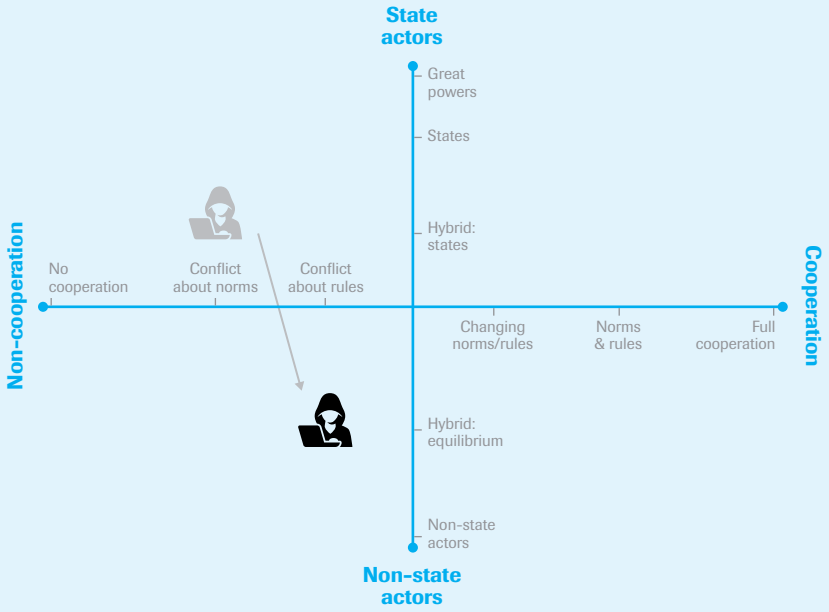
Given the lack of international regulations in the area of cybersecurity, it is difficult to say anything about compliance with existing rules. The agreements made in regional organisations are also generally non-binding and are not verified. Verification of behaviour in cyberspace is an extremely complicated process anyway because, unlike physical weapons, computer codes are, after all, easy to hide. The UN working party's confirmation that international law integrally applies to the cyber domain is an important step, but it is still unclear how it must be applied in practice and how compliance can be monitored.

The quadrant chart and shocks

The international regime for the cyber domain is still being developed: there are as yet no shared norms and absolutely no rules whatsoever. At the moment, there are (serious) conflicts in the regime about the underlying norms. There is as yet no effective cooperation between the large number of state and non-state actors. There is very little movement visible in the position on the quadrant chart (see Figure 4), although by 2021 it can be expected that there will be somewhat more consensus about the key norms, and parties will be working to draw up somewhat more rules. However, it is still uncertain whether this will be successful.

21 Charney, S., et al. 2016. 'From Articulation to Implementation: Enabling progress on cybersecurity norms', *Microsoft*, https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity Norms_vFinal.pdf.

Figure 4 The international regime: Cybersecurity (2016-2021)



However, expected trends in the cyber regime can also be changed by sudden events. To allow for such changes, the Clingendael Expert Survey also identified and graded a number of possible events for this system of cooperation (see Figure B). A number of possible shocks emerge from the expert survey that can cause a change in international relations in the cyber domain. An acceleration of the existing cyber arms race was specified as being the most probable, certainly if linked to a possible increase in cooperation between the business sector and states on this level. Although the current major powers (led by the US, China and Russia) now also seem to be leading the way in the cyber arms race, other countries may join the list of cyber superpowers in the years to come. Another possible shock is that Western technologies start to lag behind those of non-Western parties. The rise of non-Western technological companies can play a role here. If the West loses its technological advantage, international relations will also change, of course. The last possible shock to be identified is a massive cyber attack on the international financial markets. Such an attack would have devastating consequences for the world economy and could also result in a shift in relations.

One shock that is not included in the expert survey but should perhaps nevertheless be mentioned is the possibility of the first large-scale military cyber operation with serious consequences. Suppose that a country were to launch a massive cyber attack on another country – for example, by crippling communication and energy systems for an

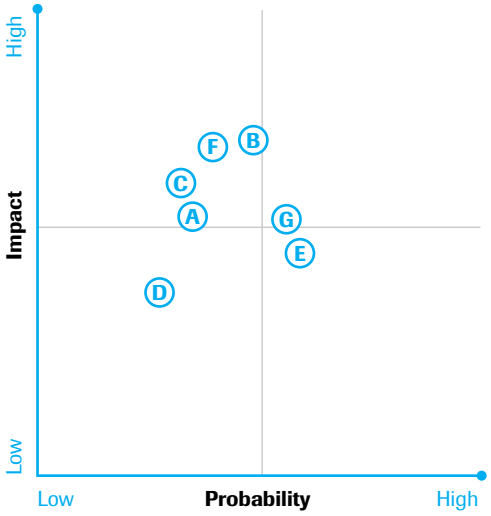
extended period – that would have a major impact on society in the country in question. The international reaction could then involve two dimensions: further acceleration of the digital arms race (with a growing risk of escalation) but also an acceleration in attempts to formulate more international rules and norms in this area.

Conclusion

Although the threat in the cyber domain is growing rapidly around the world, the international community still has not found an effective way of dealing with it. Due to various problems, such as divergent views and the huge importance of non-state actors in the cyber domain, international cooperation is still on a relatively low level. This means that the threat will also not diminish from this perspective. And the significant growth in the digitisation of the global society means that the threat will only increase. It is possible that attacks with a major impact will have to be launched before international willingness to cooperate becomes more urgent. The absence of such incidents could lead to years of muddling during which many smaller-scale cyber incidents occur, but countries and organisations continue to take countermeasures individually.

Appendix: Figures

Figure A Possible shocks related to the threat assessment for cybersecurity (N=11)



A Ground-breaking breakthrough in the field of energy results in a significant reduction in the world's dependency on fossil fuels

B Enormous Russian cyber attack

C More advanced autonomous weapons systems

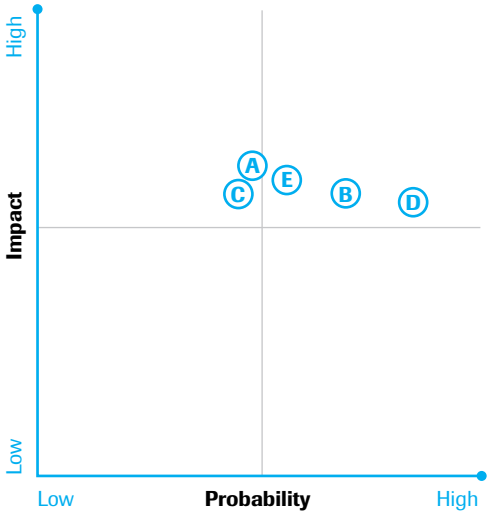
D Negative consequences of 3D printing

E Negative consequences of robotics

F Uncontrollable nanotechnology or biotechnology causes large-scale, serious damage to human beings and the environment

G Technological advances in the weaponisation of space

Figure B Possible systemic shocks related to cybersecurity (N=11)



A Large-scale cyber attacks on the financial system

B Large technology companies working more and more with government agencies on cybersecurity

C Non-Western technology giants become dominant

D Government agencies gradually invest more and more in cyber war

E Superiority of Western technology is negated