CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Ten Rules for Cyber Security

Eneken Tikk

This article was first published in Survival | vol. 53 no. 3 | June-July 2011 | pp. 119-132

Since the large-scale cyber attacks on Estonia's government, telecommunications infrastructure, banks and online media in 2007, the global perception of cyber threats has drastically changed.[1] Politically and ideologically motivated cyber attacks on critical infrastructure have been a wake-up call for security experts and have shown there is a price to pay for an advanced information society. More recent cases such as Aurora (the 2010 attacks against Google and other corporations in China), Conficker (a computer worm targeting Microsoft Windows, detected in 2008) and Stuxnet (a worm targeting the Iranian nuclear programme) show that cyber crime continues to increase in sophistication.[2]

Before the Estonian incident, organisations tended to treat their risks and arrangements in isolation. Cyber security was merely the sum of individual contingency plans having little to do with more systemic risks. What coordination of defences existed involved developing uniform and standard solutions rather than plans or capabilities for coordinated action. Since 2007, however, the United Nations, NATO, the European Union, OSCE and other international organisations have introduced new cyber-security policies or revised existing ones. The concept of cyber crime has been expanded; Estonia, for example, amended its penal code to criminalise computer crime against critical information infrastructure as well as cyber terrorism.[3]

Other areas of policy and law, beyond cyber crime, also need to be adapted to the new threat situation. Attacks with national-security impli-

Eneken Tikk is Legal Adviser at the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

cations test the limits of the existing legal framework for data protection, electronic communications and access to public information. Moreover, nations are already developing cyber-warfare capabilities. The spectrum of cyber conflict ranges from breaches of internal policy or regulations (not patching software, for example) to breaches of legal obligations (such as not reporting illegal activity) to crime to national-security threats to outright cyber warfare ('cyber armed attack'). The levels and sources of law relating to cyber security range from the soft (standards and best practices) to organisational (contracts and internal regulations) to national to international agreements and customary law, which inform the four key legal areas the law of network and information security (also referred to as cyber law or information-society law), dealing with, for example, data protection, e-commerce, electronic communications and access to information; criminal law (offences, investigation, cooperation); national-security law and possible restrictions to human rights and liberties resulting from national-security concerns; and the Law of Armed Conflict.[4] The spectrum of conflict parallels, but does not coincide perfectly with, the spectrum of legal frameworks and remedies.

Cyber attacks test the limits of existing law

Contemporary cyber threats can only be confronted by combining the regulation, remedies and legal practice these four key areas of law. Ten rules focused on issues and working solutions arising from discussions among experts or in the course of cyber-incident handling can be identified.[5] These offer an abstract but concentrated view of the legal issues affecting the handling of cyber incidents and cyber security in general, and highlight the disparity between legal theory and practice. The rules are intended to focus international debate on the quality and interpretation of existing law rather than the need for new legal frameworks. Several issues sometimes considered as legal, such as attribution, identification or criminal cooperation are, as a matter of fact, related to political or technical aspects and need to be considered from the perspective of constructive solutions. Several issues seen as challenges for new legislation, for example data protection or Internet service-provider

(ISP) liability, can, moreover, be solved through interpretation of or simple exceptions from existing legal constructs instead of a wholly new legal approach.

The Territoriality Rule

> Information infrastructure located within a state's territory is subject to that state's territorial sovereignty.

In view of the global nature of cyber threats, there is on-going debate over whether territoriality-based legal frameworks can cope, but the lessons of Estonia, Georgia and other major cyber incidents show that nations can and must make better practical use of the legal remedies and concepts available under national law by fine-tuning their national regulations. Electronic communications, criminal sanctions, investigative authority, cooperation with ISPs and many other essential elements of successful cyber defense depend on the quality of the national law. Until the options for implementation and interpretation of national legal instruments are exhausted, it is difficult to determine what, if any, remedies need to be agreed upon on the international level.

Cyber infrastructure is subject to the jurisdiction of the flag state and is subject to the sovereign prerogatives of that state. Every government can exercise effective control over the IT infrastructure located on its territory, for example by ensuring the availability and quality of logs, maintaining an overview of the providers of electronic communications, developing an understanding of threats and capabilities existing within its jurisdiction to cope with and manage incidents, and balancing the development of the information society with the interests of national security.

The territoriality principle empowers nations to impose their sovereignty on information infrastructure located within their territory or otherwise subject to their jurisdiction. The responsibility of a state for securing its own networks is supported by the internationally recognised concepts of non-intervention and sovereignty.[6]

The Responsibility Rule

> The fact that a cyber attack has been launched from an information system located in a state's territory is evidence that the act is attributable to that state.

If a cyber operation has been launched or otherwise originated from governmental cyber infrastructure, there is a rebuttable presumption that the state in question is associated with the operation. Nations therefore need to consider the potential that they could be held responsible for attacks or other activities that make use of their information infrastructure. They will face public condemnation and will be expected to respond and assist with investigations. Information leading to the identification of the source of an attack or about the perpetrators, methods and tools involved, and even active law-enforcement measures such as confiscation, arrests and prosecution, should reasonably be expected from the countries whose infrastructure has been involved.

In 2007, for example, Tallinn accused Moscow of cyber attacks against criticial Estonian government and private infrastructure networks. This attribution was based, among other things, on Russia's refusal to cooperate in attempts to uncover the details of the attacks. Russia has also been associated with the cyber attacks against Georgia and Lithuania in 2008.[7] China has similarly been accused of launching cyber-espionage attempts against the United States' and other nations' information systems.[8]

Countries may also be expected to raise their own levels of cyber security by establishing stronger control over the use and exploitation of the information infrastructure under their jurisdiction. The balance between economic and security interests will, of course, need to be struck on a case-by-case basis.

The attribution principle has little support in current international law on state responsibility. The two key standards are effective control and overall control. According to the 1986 Nicaragua case, effective control (financing, organising, training, supplying and equipping as well as the selection of targets and the planning of the whole of an operation) is not enough to meet

the threshold.[9] In the 2003 Tadic case, it was concluded that overall control goes beyond the mere financing and equipping of forces and involves participation in the planning and supervision of military operations.[10] Constructs for attribution where evidence of immediate involvement is lacking are known in international environmental law.

The Cooperation Rule

> The fact that a cyber attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state.

The interconnectedness of global information infrastructure makes it impossible for any nation to defend itself against cyber attack without cooperating with states whose infrastructure can be used to route such an attack. More effective cooperation is needed between public and private institutions as well as between national governments and international organisations. Cross-disciplinary cooperation between legal, policy, military and technical experts is also necessary.

While the vast majority of information infrastructure is privately owned and operated, there is significant dependence on public information services and networks that the private sector supports on a contractual basis. Cooperation may take the form of consulting, information exchange and reallocation of resources, as well as supporting services under attack. National provisions on ISP cooperation, data exchange and partnerships as well as coalition agreements will support the legal framework for cooperation. The Cyber Crime Convention invites the parties to cooperate through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[11] The cooperation principle can also be found in the North Atlantic Treaty,

whereby the parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the parties is threatened.[12]

The Self-Defence Rule

> Everyone has the right to self-defence.

The concept of self-defence is part of both criminal and international law. In principle, everyone has the right to self-defence, subject to the proportionality and necessity of such action.

In criminal law, if victim reasonably believes that unlawful force is about to be used against him, there is no liability for what would otherwise be wrongful acts in self-defence. This is not say that every cyber 'hack-back' can be justified under the concept; it should be a remedy of last resort.

On the international level, the criteria for invoking individual and collective self-defence are based on custom, the UN charter and international case law. A cyber attack invokes individual and collective self-defense if it rises to the threshold of an 'armed attack'. The assessment of whether a cyber attack is, by its effects, consequences or nature, is equivalent to such an attack will be made by national authorities or, for collective action, by international partners (the North Atlantic Council invoking Article V of the NATO Treaty, for example). According to Article V, an armed attack against one or more of the parties in Europe or North America shall be considered an attack against them all and, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the UN Charter, will assist the party or parties attacked.[13]

So far no cyber attack has crossed this threshold and no military response has yet been made to a cyber attack. A kinetic response in self-defence against a cyber attack can be legal if it is necessary put an end to the attack and the response is proportionate to the method and impact of the attack.

The Data Protection Rule

> Information infrastructure monitoring data are perceived as personal unless provided for otherwise (the prevalent interpretation in the EU).

The need for network monitoring and information exchange has to be carefully assessed against individuals' right to privacy. There is currently a considerable divide between the legal and technical approaches to data and their security.[14] While the monitoring of network data seems to be well-established and routine in technical communities, it raises significant concerns among legal experts.

According to the EU Data Protection Directive,[15] any information relating to an identified or identifiable natural person is regarded as personal data. The prevalent opinion in the countries implementing the directive is that IP addresses are personal data and subject to processing restrictions under national legislation.[16] Such restrictions include requiring the consent of the data subject for processing these data, prohibitions on transferring these data to third countries, and potential inadmissibility as evidence of such data obtained in an unlawful manner. According to the EU Data Protection Directive, the transfer to a third country of personal data may take place only if the third country ensures an adequate level of protection.[17]

These prohibitions can inhibit attempts at the national level to identify, attribute or prevent cyber attacks, but the directive allows for exceptions in the public interest and for national security. There are also exceptions for criminal proceedings. Clearly identifying the need for and methods of data and packet inspection will help establish the right balance between privacy and monitoring.

The Duty of Care Rule

> Everyone has the responsibility to implement a reasonable level of security in their information infrastructure.

The concept of duty of care is well established in many areas of law: an individual is under obligation to guarantee the protection of personal data he

processes, and due-diligence duties arise from the legal framework of data protection, information-society services, consumer protection and so on.

Under the EU Data Protection Directive, for example, a controller of personal data must implement appropriate technical and organisational measures to protect such data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, taking into account the state of the art and the costs of implementation.

A similar floating standard is set in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). Article 7 requires appropriate security measures to be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

As cyber threats with political dimensions become more prevalent, the duty of care concept can be extended to develop security standards for critical information infrastructure and governmental or military information services.

The Early Warning Rule

> There is an obligation to notify potential victims about known, upcoming cyber attacks.

In 2008, 300 Lithuanian websites were defaced with the hammer and sickle symbol after the Lithuanian Parliament passed a law banning (among other things) the use of Soviet symbols. The attack itself involved a single, easily fixed ISP vulnerability, but the response had broader ramifications**:** having learned of the upcoming attacks, the ISP issued an early warning to its customers and informed them about the incident.[18] If implemented widely, this approach could considerably improve cyber security.

The fact that governmental agencies were given advance warning of the attacks highlights the standards for service-level agreements (SLAs) for governmental information infrastructure and the need for a non-discriminatory duty to inform both public- and private-sector ISPs and web hosts about known threats.

The issue of SLAs is, to a great extent, a matter of national legislation or contracts. For Lithuania as well as other European Union members, the obligations of service providers to ensure security of services derive from the ePrivacy Directive EC/2002/58.[19] This directive invokes a general obligation to take appropriate technical and organisational measures to safeguard the security of a provider's services. If necessary, the service provider must coordinate further action with the provider of a public communications network to which it connects. According to the E-Commerce Directive, member states may establish obligations for information-society service providers promptly to inform the competent public authorities of alleged illegal activities.[20]

The Access to Information Rule

> The public has a right to be informed about threats to their life, security and well-being.

There is a strong trend in Europe towards transparency of governmental acts and records, giving the public the right to be informed about threats and decisions related to their life and well-being. A holder of information is required to disclose existing information to danger to the life, health and property of persons.[21]

The presumption is that public-sector information should be publicly accessible unless there are compelling reasons otherwise. While access to information can allow the public to learn of threats and attacks and can raise awareness about cyber security, it may also result in unwanted publicity.

Private-sector organisations worry that disclosure of cyber attacks against them, and their results, might reduce trust in their business model or services. But government responses to politically motivated cyber attacks

often require publication of such information. A balance needs to be struck between these public and private-sector interests. Open discussion of the details of methods, targets and effects of an attack may also increase vulnerability, as it can tell the attackers things they would not otherwise know.

The legal framework for access to information will be an important aspect of cyber security in the context of strategic communication and public awareness.

The Criminality Rule

> Every nation has the responsibility to include the most common cyber offences in its substantive criminal law.

The criminality rule is a reminder rather than something qualitatively new. It is well established in criminal law that cyber attacks can only be investigated and prosecuted if those acts qualify as criminal offenses.

It is therefore practically impossible for the state to sanction someone engaged in a cyber attack unless the specific activity or outcome is specified as a crime under national law. Politically motivated cyber crime is for the most part a threat to society in general rather than to specific persons or entities, and may require a different response than economically motivated cyber crime.

The Lithuanian case showed that random private-sector targets can come under cyber attack as a result of political tensions. The Estonian case showed that, in a country with a rather low rate of cyber crime, politically motivated distributed-denial-of-service attacks can nevertheless effectively disrupt communications within and with the government and leave national law-enforcement agencies empty-handed, even where they have sufficient investigatory powers. The Georgian case showed how seamless connections between patriotic hackers and a government conducting kinetic warfare can contribute to the military effort with no effective legal remedy.

Existing international agreements, such as the Council of Europe Convention on Cybercrime,[22] are a good starting point for enhancing and harmonising national legal responses to cyber crime. Each party must adopt

such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.[23]

The Mandate Rule

An organisation's capacity to act (and regulate) derives from its mandate.

The mandate rule is relevant for defining and coordinating international efforts in global cyber security. Its particular, practical importance lies in the realm of developing new or revising existing cyber-security agendas.

Analysis of existing legal and policy instruments related to cyber security reveals overlaps and gaps in international coordination.[24] For example, international cyber-crime harmonisation has been a focus of at least six major international organisations. For states party to a number of such organisations, this raises the question of the appropriate input of each to a national cyber-security framework.

To justify governmental investments in their cyber capabilities, international organisations should make use of and enhance the efforts of other entities. While NATO's primary focus in the field, for example, could be on mechanisms for collective self-defence, it still needs an framework for handling cyber incidents below the threshold of a 'cyber armed attack', whether targeted against the organisation itself or an individual member states. Cyber defense is many times more costly than mounting a cyber attack, and as governmental information infrastructure becomes a more frequent target, developing national and international capabilities will become an investment issue. NATO's niche could be gathering, exchanging and developing best practices for dealing with cyber attacks with national-security consequences or issues of cooperative defense and security.

* * *

These ten rules outline key concepts and areas that must be included or addressed in a comprehensive legal approach to cyber security. They are

intended to raise awareness about existing legal complications involving cyber security and the ways to overcome them, to serve as a focus for debate and coordination within and across disciplines, and to inform well-grounded proposals for additional legislation on the international level.

Notes

1 For details about the 2007 attacks and the legal considerations involved, see Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: CCD COE Publishing, 2010).

2 For Operation Aurora see http://www.damballa.com/research/aurora/; for Conficker see http://www.Confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage; for Stuxnet see Nicolas Falliere, Liam O Murchu and Eric Chien, *W32.Stuxnet Dossier*, Version 1.3 (November 2010), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, p. 4.

3 For details about the Estonian legal lessons learned and amendments to national laws, see Kadri Kaska, Anna-Maria Talihärm and Eneken Tikk, *Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007*, International Cyber Security Legal and Policy Proceedings (Tallinn: CCD COE Publishing, 2010), pp. 40–67.

4 See the 2009 Cyber Conflict Legal and Policy Conference organised by CCD COE. The agenda of the Conference is available at http://www.ccdcoe.org/legalconference/.

5 At the 2010 CCD COE Cyber Conflict Conference, four legal areas – data exchange, state responsibility, criminal cooperation and the applicability of international law – were addressed by legal experts from at least two key areas (data exchange from the cyber law and criminal law perspective, criminal cooperation from the criminal law and national-security law perspective, and so on), with the intent to identify gaps between these areas of law and come up with proposals on how to improve the existing legal framework. The agenda of the conference is available at http://www.ccdcoe.org/conference2010/agenda.html.

6 UN General Assembly Resolution 1514, at 67, UN GAO R, 15th Sess., Supp. No. 16, UN Doc. A/4684A, 14 December 1960.

7 Tikk et al., *International Cyber Incidents*.

8 See, for example, Dan Goodin, 'India and Belgium Decry Chinese Cyber Attacks', . *The Register*, 8 May 2008, http://www.theregister.co.uk/2008/05/08/belgium_india_china_warnings; John Leyden, 'France Blames China for Hack Attacks', *The Register*, 12 September 2007, http://www.theregister.co.uk/2007/09/12/french_cyberattacks; Rhys Blakely, Jonathan Richards, James Rossiter and Richard Beeston, 'MI5 Alert on China's Cyberspace Spy Threat', *Times*, 1 December 2007, http://business.timesonline.co.uk/tol/business/

industry _sectors/technology/article2980250.ece.

9 1984 ICJ REP. 392, 27 June 1986.

10 Case No. IT-94-1 (International Criminal Tribunal for the former Yugoslavia, 1995).

11 Cyber Crime Convention, Article 23.

12 Article IV of the North Atlantic Treaty.

13 Article V of the North Atlantic Treaty.

14 See Eneken Tikk, *IP Addresses Subject to Personal Data Regulation,* International Cyber Security Legal and Policy Proceedings (Tallinn: CCD COE Publishing, 2010), pp. 24–39.

15 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050. Available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

16 See Tikk, *IP Addresses Subject to Personal Data Regulation*.

17 EU Data Protection Directive 95/46/EC. Article 25(1).

18 For an overview and legal assessment of the Lithuanian incident, see Tikk et al., *International Cyber Incidents*.

19 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002 P. 0037 – 0047. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

20 EU E-Commerce Directive, Article 15 (2).

21 Estonian Public Information Act, para. 28(1) 7.

22 The Council of Europe Convention on Cybercrime (ETS 185, signed on 23 November 2001, entry into force on 1 July 2004), aiming to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction, is open for signature by the member states and the non-member states which have participated in its elaboration and for accession by other non-member states. As of December 2010 the total number of signatures not followed by ratifications was 17; the total number of ratifications/accessions was 30 (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Macedonia, Ukraine and, as a non-member, the United States). Available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

23 Council of Europe Cyber Crime Convention, Article 2.

24 For an overview of current international legal and policy instruments on cyber security, see Eneken Tikk, *Frameworks for International Cyber Security: Law and Policy Instruments* (Tallinn: CCD COE Publishing, 2010).