Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective

Eneken TIKK[1]
Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
Head of the Legal Task Team
eneken.tikk@ccdcoe.org

Introduction

About a year ago, NATO adopted two documents that will shape the way cyber incidents of concern to (inter)national security will be managed.[2] The cooperative aspect of managing cyber incidents of relevance for NATO will require national regulatory action in regard to defining the critical information infrastructure and providing a proper legal basis for information exchange between NATO and its member states.

Cyber incidents may range anywhere from simple deviations from internal security regulations to criminal acts, acts of cyber terrorism, and even warfare. The investigation and management of such incidents is based on sharing and comparing traffic data and server logs, including IP addresses. Countries subject to both the EU and NATO organisational framework of cyber defence[3] will face difficulties transferring such data to NATO or another member state's national authorities since the legal view governing EU data protection institutions categorises IP addresses and logs as personal data.

The EU legal framework on data privacy thus creates obstacles to processing cyber incident data for the purpose of cooperative cyber defence management. While there are legally safe ways to secure evidence and manage cyber incidents, recent trends in EU member states require that more attention be paid to these issues on the national regulatory level.

---

[1] *Eneken Tikk works as the Legal Advisor to the NATO Cooperative Cyber Defence Centre of Excellence ("CCD COE") and is currently the Research Fellow for the Center for Infrastructure Protection of the George Mason University Law School.*

[2] NATO Cyber Defence Concept (MC, 13 March 2008), based on the NATO Cyber Defence Policy (NAC, 20 December 2007).

[3] While there is no internationally accepted legal definition of cyber threats (one of the key reasons for difficulties related to the implementation of personal data protection rules), the concerns of cyber security involve stakeholders such as international organisations, governments, the private sector and IT infrastructure providers, as well as home users. The incidents that may affect the functioning of a society's critical infrastructure may initially occur as simple human error and the deviation from internal information security regulations, or they may turn out to be intentional, often politically motivated, criminal activities or coordinated and well-targeted attacks that support other hostile activities towards the entity or nation in question. Therefore, the term "cyber defence" is to be understood to cover the prevention of and potential responses to different types and levels of cyber threats.

This article will provide insight into personal data protection issues that relate to the exchange of information concerning cyber incidents and, based on considerations pertinent to national approaches, it will provide guidance on how to minimise the related legal risks that come with cyber incident management.

1. The Benefit of Sharing Information

During 2007 and 2008, the CCD COE legal team analysed the legal aspects of five major cyber incidents – Estonia, Radio Free Europe in Prague, Lithuania, Georgia, and Burma[4].

The Estonian cyber incident that occurred in early 2007 was a landmark case, where publicly sharing information about the cyber attacks turned out to benefit the government in its efforts to defend itself against its invisible enemy. Since then, major IT security think tanks and international media channels keep a column on cyber incidents of international concern.

There is an increasing amount of information available about politically motivated and government-targeted cyber incidents. The management of cross-border cyber incidents and conflicts, however, requires extensive and detailed information-sharing among governmental entities and also among these last and the entities responsible for the information infrastructure, which are often privately owned. This kind of cooperation is inevitable between nations and international organisations.

The data of interest comprises not only details about the course of action and background of the incidents but also real-time reporting on targets and, most importantly, details of the server logs, which make it possible to differentiate the good traffic from the bad, block hostile IP addresses, and trace the origin of the attacks.

With cyber defence developments in NATO, sharing information on cyber incidents will form an essential part of the national cyber security agenda. The study of recent cyber incidents shows that the nature of the information infrastructure[5] in conjunction with the territoriality principle[6] make it difficult for a nation, when acting alone, to defend itself against cross-border cyber attacks.

NATO has developed a mechanism to assist nations in case of severe cyber attacks, but the implementation of the relevant provisions of the Cyber Defense Policy and Cyber Defense Concept requires structured and well-coordinated information sharing on those aspects that demonstrate the relevance the said cyber incidents have for NATO.

In order to meet the criteria for receiving help from rapid reaction teams, consulting or any other type of assistance, the nation must satisfy a burden of proof of the relevance of the conflict for NATO. This can only be done after a thorough analysis

[4] These papers are available on www.ccdcoe.org.

[5] The nature of the information infrastructure can be best explained by the rationale that was employed in developing the Internet. It was designed as a response to national security concerns to provide a communications network that would work even if some of the sites were physically destroyed. If the most direct route was not available, routers would direct traffic around the network via alternate routes.

[6] The contemporary legal framework adheres to the concept of sovereignty, which is granted to the nations on the basis of the physical dimensions of their air, land and sea territory. While few other arrangements exist (the common understanding of governing high seas and space), so far no general agreement has been concluded with respect to the governance and control of the Internet. Therefore, conduct on the Internet can only partly and conditionally be subjected to a nation's jurisdiction.

of the underlying facts about the nature, extent and sources of the incident has been completed.

In summary, effective defence relies on cooperation, and effective cooperation needs precision in terms of facts of the incidents. Effective measures of defence depend on accuracy of information and in order to achieve prosecution, the evidence must be able to indicate the source of the attacks.

Estonia is one of the countries that is both a NATO nation and an EU member state. In the context of cyber security there is an increase in the interrelation of the activities and areas of concern for these two major and influential organisations; sharing information on cyber incidents is just one of them.

2. EU vs. NATO: The Cyber Security Agenda

A sustainable information society and trusted environment for e-commerce and information society services has been a key concern for the EU over the past decades. The EU is known for its wide-reaching and effective information society regulation[7], which is reflected in the national legal systems of not only EU member states but also EEA countries and others.[8]

NATO is known as a security and defence organisation, which focuses on issues that in practical terms remain beyond the scope of the applicability of the EU law. The "security" paradigm has been changing over the past couple of decades, expanding the focus of defence interests beyond kinetic and symmetric threats to include issues such as terrorism, electronic warfare and critical infrastructure protection.

---

[7] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24/04/2002 pp. 0033-0050; and four specific Directives: Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector).

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 (Personal Data Protection Directive); OJ L 281, 23/11/1995 p. 31; 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); OJ L 201, 31/07/2002 pp. 0037 – 0047.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178 , 17/07/2000 pp. 0001–0016.

Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was published in the Official Journal of the European Communities; OJ L 13, 19/01/2000, p. 12.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information; OJ L 345, 31/12/2003 pp. 0090–0096.

[8] Currently, personal data can flow between the 27 EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) and to Switzerland, Canada, Argentina, Guernsey, and the Isle of Man. An exception is granted to the US Department of Commerce under the Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection.

Thus, in the past few years, the interests of these organisations have developed significant overlaps. This is especially the case since NATO has begun to look more into the cyber attacks and has recognised that not only cyber incidents against military targets but also those directed against national governmental and possibly private critical infrastructure functions may affect (inter)national security, thus deserving the interest of this military organisation. It is due to this interest that a common playing field has emerged for the two organisations.

While the two organisations share interest in the field of Critical Infrastructure Information ("CII") protection, personal data protection in the EU legal framework may become a factor that could hinder the creation of effective cyber defence, unless timely and duly attended to by the interested nations and entities.

There seems to be some inconsistency in the application of the Directive 95/46/EC (herein after referred to as 'the Directive' or 'the 'Personal Data Protection Directive') by the Member States. These differences in interpretation and application of the Directive are particularly evident when looking at the approach taken by Germany in comparison with Sweden. These two cases will be discussed below. The dominant view held by the EU data protection authorities, however, requires that information sharing regarding cyber incidents be supported by specific legal provision under the national law of each Member State.

3. EU data protection agenda and reflections on member states

Systematic data protection in Europe dates to the aftermath of the Second World War and arises from the need to face the threat that people could be potentially mistreated based on an abuse/misuse of personal data available to the state. [9] Essentially, the EU data protection regulatory framework is based on the prohibition of processing personal data and has issued different exceptions that allow the data to be processed under a set of personal data protection principles and restrictions.

Directive 95/46/EC serves as the basis for personal data protection legal acts in nearly 30 advanced information societies. Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by

[9] In 1939, the German authorities conducted a census to register German Jews and those who were half Jewish with the *Reichssicherheitshauptamt*. While the authorities claimed that personal data, such as religious inclination and nationality, were confidential, a national registry was created on the basis of those data to point out which citizens had a Jewish parent or grandparent. Similar registries were created and updated in Poland and compared to the data of the 1933 census. After the census, the German citizens were listed in the *Reichskartei* as Aryans or non-Aryans and their fate for the purposes of the Second World War was determined by the Nazi authorities controlling those registries.
In this context, the statistical data was put to the service of the governing regime. Extremely high regard to population policy transformed normally quantitative data about people into a qualitative and psychological basis of reigning. Although statistical in nature, this information relied on the penetration of private and public lives, recording and categorising such data, and last but not least, subdivision of the data.
The census based on religion and nationality were not the only listed categories of information. In 1935, the authorities created the labour registry, in 1936 the health registry, in 1939 the population registry, and in 1944 the personal identification number system. From 1934 on, those with hereditary illnesses were registered. By the beginning of the war, the authorities had a clear picture of family planning, land inheritance and health status of the population. These statistics were put to service by and under the control of the authorities.

reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a).

This definition is intended to be extensive. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link themselves. Some examples of "personal data" are: address, credit card number, bank statements, criminal record, etc.

Recently, EU data protection supervisor, Peter Hustinx, shared his opinion on IP addresses as personal data, pointing out that IP addresses are also protected under data protection laws. Speaking to ZDNet at an RSA information security conference in London, he said that a person does not have to be identifiable by name in order for details of computer usage to be protected. Companies that gather addresses that might or might not be personal data should just treat them all as personal. When companies are unsure whether information, such as activity or server logs or a record of Internet protocol (IP) addresses, are personal data or not, they should treat it all as personal data.[10]

In the event personal data is treated, any processing[11] of such data falls under the jurisdiction of the Directive unless it has otherwise been provided for under national law.

In the context of information exchange regarding cyber attacks, one of the more important provisions of the EU Data Protection Directive in the context of exchange of information about cyber attacks is Article 25, which prohibits the transfer of personal data to third countries.[12] In principle, the transfer of personal data to countries outside of the EU requires the European Commission to assess the specific personal data protection regulations and practices of the country concerned.

Since cyber threats have affected different countries, the national courts have the task of providing guidance on how to deal with those threats in the context of personal data privacy concerns. Interestingly, the views and approaches to the balance between privacy and security expressed by the various national courts indicate not only a difference of position and approach from country to country, but it also highlights the existing challenge of finding a balance for the application of the directive itself.

In a verdict of 27 February 2008[13], the *Bundesverfassungsgericht* (German Constitutional Court, henceforth "BVerfG) ruled that from the right to personal self-determination comes an individual's right to security and integrity of information

---

[10] Michael, James. EU DP Supervisor says IP addresses are protected. Privacy Laws and Business International Newsletter, December 2008, issue 96, page 9.

[11] Under Article 2 (b) of the Directive, processing personal data ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

[12] The Member States shall provide that the transfer to a third country of personal data, which are undergoing processing or are intended for processing after transfer, may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectorial, in force in the third country in question and the professional rules and security measures which are complied with in that country.

[13] http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

systems (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). The essence of this ruling reflects Germany's well-established guarantees of personal privacy, privacy of communications, and protection of personal data, and it emphasises the duty to refrain from violating the privacy of the user without a proper basis in applicable law.

The court emphasised that covert infiltration in information systems resulting in the surveillance of a person's use of that system is only allowed when there is a) effective evidence, b) a real threat, c) a legally protected value, and d) where the authority for such interference is clearly provided for in the law. This effectively provides a relevant authority with a checklist of legal criteria/conditions that must be met in order to carry out a surveillance procedure. The court specified that threats to the fundamental institutions or existence of the state itself would indeed be a category that could justify such interference, indicating, *inter alia*, that under certain circumstances surveillance can be justified as a pre-emptive measure. In addition to the factual and legal necessity outlined above, and as part of the legal basis of authority requirement (element d) also referenced above, resorting to such measures in Germany would usually also require a court order as a prerequisite.

BVerfG represents a cautious approach to how and to what degree the authority of the state has over private communications and in particular the surveillance of such communications.

As such, the judgement in Germany is in counter position to recent developments under Swedish law, where a bill was passed in June 2008 that allowed for monitoring of all emails, text messages and phone calls for the purpose of national security.[14] This legal instrument received widespread public criticism for excessively restricting civil liberties, violating integrity and creating a "big brother" state. According to the law, the state institution given the authority for surveillance, FRA (*Försvarets radioanstalt*, the Swedish National Defence Radio Establishment) – unlike the police – would not be required to seek a court order to commence surveillance[15]; however, the Swedish Data Inspection Authority would supervise the activities of the FRA, and a collective board would be instituted to decide on surveillance in specific cases.[16]

The UK Information Commissioner's Office (ICO) has issued a statement that isolated IP addresses do not constitute personal data, but become personal data if they are used to create a profile on an individual or when in the hands of an ISP. According to the ICO's reasoning, it is difficult to use IP addresses to build up personalised profiles. Many IP addresses, particularly those allocated to individuals, are 'dynamic'. This means that each time a user connects to their internet service provider (ISP), they are given an IP address, and this will be different each time. So if it is only the ISP who can link the IP address to an individual it is difficult to see how the Act can cover collecting dynamic IP addresses without any other identifying or distinguishing information. Some IP addresses are 'static', and these are different. Like some cookies, they can be linked to a particular computer, which may then be linked to an individual user. Where a link is established and profiles are created based on static IP addresses, the addresses and the profiles would be personal information and covered by the Act.

[14] 'Signal Surveillance Act', Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet
[15] 'Yes' to surveillance law. The Local, June 18, 2008. <http://www.thelocal.se/12534.html>
[16] Thelenius-Wanler, Emma. Riksdagen röstade igenom FRA-lag. Dagens Nyheter, June 18, 2008. <http://www.dn.se/DNet/jsp/polopoly.jsp?d=147&a=795317>

However, it is not easy to distinguish between dynamic and static IP addresses, so there is limited scope for using them for personalised profiling.[17]

The ICO approach is a purpose-based approach, where the applicability of the Directive would depend on whether processing the data is intended to justify the aim of the Directive itself or not. However, in light of personal data protection regulation in the EU and the numerous rulings of the European Court of Justice and the European Court of Human Rights, the focus of the Directive may have shifted towards a German school of interpretation.

Furthermore, the EU data protection authorities have recently supported a rather protective approach towards personal data protection. Thus, the personal data protection regulation under the First Pillar may have a cooling effect on the implementation of measures regarding Third Pillar concerns and more generally, affect the way that the world manages cyber incidents.

4. Balancing Privacy and Cyber Security

In the hierarchy of fundamental rights, the right to privacy has traditionally been considered one of the most significant, coming right after the "vital" rights to life, health, and freedom.[18] As long as there are security concerns regarding these legally protected values, creating exceptions from the Directive may be seen as a matter for national regulation.[19]

But contemporary cyber incidents are often difficult to legally categorise. The Estonian cyber incident, often referred to as Cyber War 1.0, did not really result in loss of life or freedom, but rather portrayed a novel set of threats that does not readily fit into the existing perception of threat. Similarly, nobody was killed or injured in Georgia as a result of DDoS attacks against government and media websites.

Modern information societies have become greatly dependent on information infrastructure and consequently may not only be vulnerable in "traditional" ways but also in the context of accuracy, reliability and security of information, not to mention those ways that could restrict the freedom of information and speech. These threats are not readily justified exceptions from the area of application of the Data Protection Directive. As a matter of fact, these threats do not fall within the focus of the law of armed conflicts or criminal law in the field of IT, either.[20]

Therefore, in order to create legal certainty for processing data about cyber incidents, the concept of cyber threat as well as the components of cyber incident management, such as transmitters and recipients of data and the nature, purpose and possible legal effect of data processing, need to be defined under the national regulatory framework.

---

[17] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf .

[18] Vital interests of the data subject or a third person are a legitimate basis for processing personal data without additional consent requirements under Article 8 (2) c.

[19] According to Article 3 (2), this Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on the European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

[20] LOAC was drafted with kinetic and bloody wars in mind, whereas most of the criminal law pertaining to IT incidents has the economic effect of IT criminality in the background.

Otherwise, different opinions regarding the applicability of the personal data protection framework may hamper legal proceedings related to cyber incident management and create even more inconsistency in implementing the measures created for this complex and sophisticated legal area.

5. National Self-Help Remedies for Personal Data Protection Risks

Under the circumstances, where the extent of cyber security exceptions under the EU Personal Data Protection Directive is unclear, the nations are in a position to consider additional regulatory steps to reduce the risk of personal data privacy invasion and to support the interaction between national CERTs, the private sector, the government and international entities dealing with cyber defence.

These include: clearly indicating and better defining the area of applicability of the national personal data protection regulation; defining the elements of critical infrastructure that, if attacked or otherwise disabled by electronic means, would be part of a member state's request for assistance to NATO; and using other, possibly technical, economic, policy etc. measures in order to shape society's tolerance and general understanding of cyber security.

5.1. Making a Provision Concerning the Area of Applicability of the EU Personal Data Protection Regulation in the Field of Cyber Security

As indicated by the BVerfG, the elements necessary to design the national view of cyber security clearly ought to provide for the aforementioned conditions of a) effective evidence of, b) a real threat against, c) a legally protected value, and d) the authority for interference.

In other words, the exceptions to the national data protection regulation have to be tied to national threat assessment procedures and legally accepted means of cyber deterrence. Last but not least, the authority must give clear indications that allow for the immediacy of a threat to be determined.

5.2. Defining Critical Infrastructure (Relevant to Cyber Security)

Defining the components of national information architecture, that are not only critical for the State to function correctly but also to preserve national security, will render the institutions that are part of the information flow transparent in case of a cyber incident of concern to national security. This will, on the one hand, establish the framework for the potential focus regarding personal data processing and thereby serve as part of the legal basis for data processing.

On the other hand, defining the components that are critical to national, and possibly international security, will outline what the potential threat assessment and risk management criteria are for the institutions involved. For example, under the Directive 95/46/EC, the private sector is under obligation to provide the data subject with a comprehensive understanding of the potential uses of the data available about him or her. The definition of CII elements will help to determine and define additional legal measures such as audit obligations, threat assessment and reporting measures or potential restrictions to terms of use of critical information systems.

5.3. Defining the Procedure for the Exchange of Information Regarding Cyber Incidents

There are a number of persons involved in gathering accurate and consistent data on cyber incidents. Provided that the addressee of the information about the incident is NATO Cyber Defence Management Authority, the information will be readily accessible to potentially all NATO nations. The information will be provided by a designated national authority that, under most circumstances, is not in the position to directly gather data, but will be enabled to use different sources, such as national CERTs, components of the CII under attack and ISPs. Last but not least, information may be directly or indirectly collected from the data subjects.

In order to minimise the risk that the information and details of the incident are not misused, the potential chain of information ought to be defined so as to create a correct legal basis for processing such details.

5.4. Engaging soft law and self-regulatory means to enhance national cyber defence capability

The law in the field of cyber defence and cyber security is evolving and is, to a great extent, dependent on political (and popular) views on the issue. It is important therefore that all legal measures be communicated to the general public from the moment that such regulation could necessitate a reduction in the sphere of privacy and anonymity of the data subject in order to ensure national cyber security. Laws regarding privacy may very well need an element of public dialogue to better support the activities of the cyber defence authorities and law enforcement agencies and to increase the understanding and cooperation of these last with the data protection authorities.

Creating an understanding between all stakeholders of the information society is a task that no government is capable of implementing on their own. Consequently, a global approach to the development of national cyber security policies and strategies must be taken that incorporate not only international concerns but also the interests of the private sector and the habits of individual consumers in the information society.

Conclusions and a way forward

The ideas presented above, which take a generalised look at national approaches into account, aim at identifying more effective cyber defence policies and strategies. As international cyber security concerns evolve, more constructive and sophisticated cooperation is needed between the EU and NATO, and potentially other international organisations, to ensure that any loose ends in the defence measures adopted are kept under control and resolved.

As countries build their national cyber defence framework, they face the privacy vs. security test. It is not only about choosing between the approaches of Germany and Sweden, which find themselves on either end of the privacy vs. security spectrum, but it is also a question of taking the factors of cyber threats unique to each nation and balancing them with the international cyber security agenda and concerns.

Recognising and defining CII as an aspect of cyber threats of national/NATO relevance will serve to facilitate the management of cyber incidents by enabling a

model and procedures to be created that are capable of addressing the incidents and any information connected to them.

In defining how personal data ought to be processed for cyber security purposes, two courses of action must be considered and pursued - transparency and visibility for the data subjects and a systematic approach to be taken by the authorities to manage cyber conflicts.

National Data Protection Authorities will play an important role in reconsidering national approaches to data processing as they take aspects of cyber defence into account. In developing their views on the implementation of the EU Directive, they may need to rethink the essence and aims of personal data protection in Europe and, thus, reshape the landscape of personal privacy.