National Security Zone in International Cyber Affairs

Eneken Tikk-Ringas

The author has worked on different areas of technology and law as attorney, adviser to numerous Estonian authorities and lecturer at several universities. After building up and later heading the Legal and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn from 2006 to 2011, she joined Citizen Lab and the University of Toronto as a post-doctoral fellow for a year, also serving as strategic cyber security adviser to ICT4Peace Foundation in Switzerland. Eneken holds a PhD in law from the University of Tartu, Estonia.

Resumo

A Área da Segurança Nacional em Questões de Cibersegurança Internacional

O artigo descreve como os interesses nacionais no plano da cibersegurança estão interligados com instrumentos jurídicos, explicando como diferentes interpretações de conceitos como liberdade de informação, cooperação internacional ou direito à privacidade são contemplados em termos de Direito internacional. Analisam-se ainda ramificações quanto a abordagens governamentais relativas ao conceito de "segurança nacional", concluindo-se que nas atuais circunstâncias de fragmentação dos instrumentos legais associados à cibersegurança e ante a inexistência de acordo quanto ao que deve ser o comportamento aceitável dos Estados no plano do ciberespaço, os governos detêm uma larga latitude de discrição jurídica quando dela se socorrem para impor as respetivas perspetivas nacionais quanto a um equilíbrio entre a liberdade e a segurança.

Abstract

This article explains how national cyber security interests are entwined into international legal instruments and explains how different interpretation of concepts like freedom of information, international cooperation or the right to privacy can occur under international law. The article discusses the ramifications of governmental approaches to shaping and furnishing the concept of "national security" and concludes that under the circumstances of fragmentation of cyber security related legal instruments and in the absence of detailed agreement on acceptable state behaviour in cyberspace governments have a wide margin of legal discretion when using international legal and policy instruments to impose their national approaches to the balance of freedom and security.

Computers and networks have come to matter strategically. The emergence of the term "cyber security" itself represents an acknowledgment that turning back from a way of life powered by information technology is no longer conceivable. Whatever we have chosen or happened to connect to the Internet over time – our governments, homes, pets and passports – we now need to secure and protect. Dozens of deliberate, politically motivated confidentiality, integrity and availability disruptions known from the recent past confirm the emergence of vulnerabilities and threats on a strategic level.

Despite developing consensus on the potentially grave and wide-spread consequences of uses of ICTs for promoting political and military goals developing strategic responses has not turned out an easy task for the international community. While several governments have successfully handled large-scale cyber incidents in the recent past, international organizations are only starting to discuss acceptable state behavior and remedies available under international law. Given the natural cyber security divide stemming from the still considerable digital divide regional organizations seem to get better traction when developing confidence building measures and consolidating best practices.

An essential factor in international cyber security discussions is the concept of national security and how it relates to international peace and security concerns. While the former describes the margin of governmental discretion over a state's internal and external affairs, the latter is a representation of collective peace and stability interests. Neither of the two is a constant.

This article looks at the implementation of selected international legal instruments from a national security perspective, emphasizing that national security derogations from seemingly agreed international values can vary considerably. It addresses national security as an essential and practical element of collective cyber risk management and emphasizes the considerable margin of interpretation that governments have, at least theoretically, under international law when it comes to choosing appropriate means and methods for cyber security.

In the first part of the article freedom of information is used as a sample showcase of national approaches to balance freedom with security. After introducing a simplified outline of the right of individuals to receive and impart information and the limitations of such freedom under international legal instruments the article elaborates on the concept of "national security" in the second part and then highlights further national security exceptions in international legal instruments to frame governmental margin of discretion in addressing uses of ICTs from a national security perspective.

The author concludes that in the absence of international consensus regarding the applicability of international law in and to cyberspace, the still pending agreement on what would constitute responsible state behavior and a conclusion of which measures are necessary to increase transparency and confidence among state actors, national governments are in charge of legal and policy tools to impose their own approaches to balancing security with freedom.

Differences to Scoping Freedom and Security

What constitutes a "national security" issue is far from agreed among the international community. In fact, the degree of imposing national jurisdiction on persons, objects and events is often subject to tension and disagreement between governments.

In the context of uses of ICTs the extent of the freedom of information currently constitutes an apple of discord among three leading "cyber powers" – the United States, Russia and China. A brief look at international regulation of free flow of information offers a good example of possible margins of interpretation. To explain some inconsistencies and confrontation around the freedom of information, a simplified look at relevant legal instruments is useful.

In 1948 the Universal Declaration of Human Rights[1] articulated for the first time on an international level everyone's right to seek, receive and impart information and ideas through any media and regardless of frontiers in Article 19. It is further acknowledged under the Declaration that in conjunction to exercising the rights and obligations, everyone has duties to the community in which alone the free and full development of his personality is possible. Therefore, in the exercise of his rights and freedoms, everyone can be made subject to such limitations as are determined by law for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.[2]

A similar construct has been introduced in the International Covenant on Civil and Political Rights[3] (ICCPR), whereby everyone shall have the right to receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice (Article 19 (2)). Article 19 (3) notes that the exercise of this freedom carries with it

1 Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948.

2 Article 29 (1) and (2).

3 Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49.

special duties and responsibilities and may therefore be subject to certain restrictions, for respect of the rights or reputations of others and for the protection of national security or of public order (*ordre public*), or of public health or morals.

The European Convention of Human Rights[4] (ECHR) of 1950 similarly provides for the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Art. 10 (1)). Art. 10 (1) adds that this freedom shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. Article 10 (2) further admits that the performance of the freedom of information may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 (2) in broad terms explains the tools at governments' disposal to regulate or *ad hoc* mitigate situations that threaten national security. While the implementation of this freedom by the signatories to the ECHR is supervised and harmonized by the European Court of Human Rights, established to ensure the observance of the engagements undertaken under the Convention, not all countries are parties to the ECHR and therefore share the same views on the exercise and limitations of the freedom of expression.

The United States has proclaimed a seemingly unrestricted exercise of the freedom of information on the Internet, referring to Article 19 of the UDHR as a premise on an international level of the First Amendment, whereby Congress shall make no law abridging the freedom of speech. While limitations to the freedom of information are imposed by the U.S. to certain harmful content and obscene materials, the U.S. legal traditions reflect relatively high tolerance for offensive political and symbolic speech.[5]

China is the most widely discussed example how governments have effectively imposed restrictions on certain Internet content and services that are readily available in all countries members to the ECHR, not to mention the U.S. Restrictions on content and free flow of information have also been imposed by, *e.g.* Belarus, Saudi Arabia, Uzbekistan, and Thailand.[6]

4 Rome (1950), 4.XI.

5 For more detail about relevant court rulings, see http://www.uscourts.gov/EducationalResources/ClassroomActivities/FirstAmendment/WhatDoesFreeSpeechMean.aspx.

6 Freedom House, 2012. Freedom on the Net 2012: A Global Assessment of the Internet and Digital Media. Available at www.freedomhouse.org.

In justification of its approach to the freedom of the Internet China has referred to another UN General Assembly Resolution[7] from 1965. In this resolution the First Committee has concluded that no State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State and that all forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned. China has referred to the cultural traditions of its society as a justification to impose restrictions to "western" flow of information.

More recently, additional arguments presented by China and Russia in defense of imposing national restrictions to content highlight the Declaration of Principles on Building the Information Society: a global challenge in the new Millennium adopted by the World Summit on the Information Society (WSIS) in 2005. This instrument, reaffirming the freedom of information as an essential foundation of the Information Society, acknowledges that the exercise of this freedom can be limited by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.[8] It is noteworthy that the mandate of WSIS was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake.[9]

This simplified outline of the freedom of information in international law illustrates the potential margins of governmental discretion in establishing a national doctrine of free flow of information. The differences between nations highlight deviating considerations and rationale for governments to regard certain issues as a matter of national security or internal affairs. Further, having in mind the rise of politically motivated and increasingly organized nature of cyber incidents, one must critically ask if the WSIS principles from 2003 still reflect the full spectrum of national and international security concerns related to the uses of ICTs. Between the First Amendment approach of the US and the Great Firewall of China there are considerable shades of gray to operate in. While most governments seem to accept that the free flow of information is subject to certain limitations, the extent and even nature of such limitations are far from common sense.

7 United Nations General Assembly Resolution 2131(XX). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.

8 Paragraphs 4, 5 and 6.

9 UN GA Resolution 158/56.

The concepts of national security, public order as well as the balance between different rights and obligations are to be set by governments, at least while any more precise international consensus and widespread state practice is pending.

Cyber Security: What's in the Word?

"Cyber security" is a word pair coined to cover aspects of uses of ICTs that in the light of incidents with large-scale effects and political context go beyond technical security. One rarely encounters this term in computer and network security jargon as "cyber" is highly indistinctive of any subject matter it potentially pertains to. After all, according to popular meaning of "cyber"[10] it can encompass unmanned aerial vehicles, military command and control systems, cars, bridges, home appliances, toys and even animals and humans with certain type of implants.

"Cyber security" in contemporary government use emphasizes a strategic need or rationale behind technically securing certain assets and functions. According to the UK's 2009 strategy "cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers. /…/ Government's ultimate goal is to enable the full benefits of cyber space for the UK".[11] More often than not it invokes strategic questions and decisions about the ends, ways and means of technical security, thus adding the national security (and potentially the international peace and security) dimension to it.

While all uses of ICTs bring up the need of technical protection, their vulnerabilities and exposure to threats and threat vectors as well as the strategic rationale and prioritization of protection from a national security perspective are different for potential military objectives, civilian objects, commodities of different criticality and goods and services of convenience. This, however, does not always follow from the use of words in national strategies and agendas of international organizations.

For some time, international community used to exploit the word to primarily reflect military security concerns and remedies. These days, national and international security concerns are equally, if not more, focused on terrorism, energy, climate and economy. Although some see "cyber" as a separate category of new security challenges,[12] it would be equally correct to regard information technology

10 According to the Merriam-Webster Dictionary, "cyber" refers to "of, relating to, or involving computers or computer networks (as the Internet)."

11 Cyber Security Strategy of the United Kingdom (2009).

12 See, e.g. Tackling New Security Challenges, NATO Briefing from January 31, 2012. Available at http://www.nato.int/cps/en/natolive/topics_82708.htm.

as a component and factor part of an increasing amount of contemporary state, industry and private functions.

Based on Wolfers (1952), Ullman (1983), Baldwin (1997), Nye (2012) and others it seems to be acknowledged that the scope and focus "national security" are not constant and that military is but one dimension of security and national power shaping today's international affairs. The realities of the Great Depression, Cold War, control over technologies and now cyber, all have raised national security concerns at their own times.

Despite the haziness of "national security", it is possible to delineate it from other interests. National security serves the fundamental and persistent interests of a nation that are expected to rise above the narrow and special interests of parts of the nation yet stay below the concern of "interests of all mankind". Therefore, exercising national security naturally conflicts with international peace and security concerns. The concept of international peace and security would counterweigh national security in cases where ambitions or action of one nation threaten the peace and security of others. The mechanisms of international peace and security related measures and decision-making have been conveyed to the UN Security Council. Uses of and concerns surrounding ICTs differ considerably depending on the geopolitical, economic and societal factors characterizing the "Information Society" in different regions and states.

One needs to note that even with the event of computer security rising to the interest threshold of national security not all concerns related to uses of ICT become a strategic issue *per se*. Wolfers (1952: 481) notes that when specific policy formulas gain popularity (as "cyber security" is today) one must carefully scrutinize such concepts to avoid permitting everyone to label whatever policy he favors with an attractive name.

A look at national input to the UN First Committee discussions on International Information Security reveals that governments are equally or even more concerned with Internet governance, CERT development and law enforcement issues than they are with politico-military uses of ICTs. It is definitely questionable if all those issues are of same strategic relevance. It is essential to observe that national security remedies present themselves as (weighed and identified) alternatives to principles and policies governing the same topic if they fall within this particular area of interest.

The importance of categorizing certain objectives and issues as relevant to national security invokes a set of legal consequences empowering governments with considerable additional discretion as to balancing freedoms with security. As Nissenbaum notes, in the face of securitized threats and times of national crises, even liberal democracies accept breaks from "business-as-usual" including: (1) reduced restraints on government powers, frequently manifested in the curtailment of civil

liberties; (2) breaks from normal democratic procedure, including government secrecy normally not tolerated by citizens and (3) steep incremental funding for security agencies and infrastructures.

The flabellum of all contemporary cyber security interests is impossible to describe in meaningful detail. A few to address would be a general disagreement between liberal democracies and the Shanghai Cooperation Organization countries as to what extent is state control justified over content and the free flow of information; a principal disagreement on how the Internet should be governed and to what extent and how the international legal instruments apply to state and non-state behavior online.

Added to it nations have different immediate concerns and interests. Some are entering the curve of growing organized cyber crime, some are just building up their information infrastructure while others have started developing and deploying information technology for military use. It is therefore challenging to find a common denominator for all national concerns.

There is, however, more and more common ground to cover. The emergence of semi-political cyber protest movements like Anonymous, persistent growth of systematic and sophisticated cyber crime, concerns of cyber conflict escalation and avoidance of collateral damage of state-sponsored cyber operations represent but a small set of issues to be settled collectively for the continuous prosperity and economic benefits of the Internet. For some countries the threat has materialized more than for others.

National Security in Selected International Legal Instruments

Assuming nations are increasingly going to make use of their sovereign right to exercise control over their area of jurisdiction and use the argument of national security to enforce their strategic goals, a peek into other international treaties will offer some ideas about the potential of such arguments.

Article 27 (4) of the Budapest Convention on Cyber Crime entitles a Party to refuse assistance under the Convention if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or if the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests. This means that at least from a purely legal perspective a state can choose not to apply the Convention in case such a decision supports its national interests.

Article 34 of the ITU Convention allows Member States to cut off, in accordance with their national law, telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.

The relevance of the ITU Convention to cyber security is currently under debate. Even if ITU is not seen as a strategic security player, an exercise of the right of stoppage of telecommunications on simply technical infrastructure level by a government may result in considerable consequences for the international community.

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Article 9 (2)) allows derogation from the provisions of this convention as provided for by the law of the Party when it constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences or is necessary for protecting the data subject or the rights and freedoms of others.

When it comes to the involvement of Internet Service Providers (ISPs) in security of services on their networks, the general exception of ISP liability is also only limited to non-national security matters. Article 3(4) of the E-Commerce Directive allows Member States to derogate from its provisions in the interests of public security, including the safeguarding of national security and defense. Considerable obligations for cooperation are established to communication providers under the Data Retention Directive.

These exceptions represent just a small selection of legal tools supporting the exercise national power over persons, events and objects constituting a national security concern. Although the legitimacy of such concerns may be and often is subject to an international debate, it will be the primary task of states to define their scope of national interests and applicable remedies to protect such interests. Laws and policies addressing critical information infrastructure represent an approach taken by several countries to identifying objects of heightened protection value.

It seems to be accepted in the international community that making uses of national security derogations requires support from national law. Only under extraordinary circumstances governments can exercise their authority *ad hoc* to characterize an incident as one of national security concern. Generally, however, it is expected that governments act transparently and adopt national laws that explain the margins of authoritative engagement n case of a threat to or breach of national security.

As observed in above considerable differences may occur in national interpretation of different tights and freedoms. Such differences are expected to be less drastic among allied, regionally and circumstantially connected state actors. Still, the currently evident cyber security divide should remind the stakeholders of the importance of uniform implementation of international legal instruments and about potential issues related to overlaps and contradictions in legal instruments.

Conclusion

How to have a free, open, peaceful and stable cyberspace is a question with security and defense on the flip side. Internationally balancing relevant interests can only go half way as it is virtually impossible to unify, prioritize and remedy national and regional issues on a global scale.

This article has used the freedom of information as an illustration of the margin of interpretation involved in implementation of international law. It has emphasized the zone of national security responsibilities between individual and corporate obligations and regional and international organizations' involvement in cyber incident handling, warning that the concept of national security may not offer a broad consensus as to its scope and accepted margins.

Further drawing the reader's attention to several provisions in multilateral legal instruments that provide for derogations from criminal cooperation, availability of telecommunication services and other rights and freedoms established on international level, the author concludes that in the absence of international consensus regarding the applicability of international law in and to cyberspace, a still pending agreement on what would constitute responsible state behavior and a conclusion of which measures are necessary to increase transparency and confidence among state actors, national governments are in charge of legal and policy tools to impose their own approaches to balancing security with freedom.

References

Baldwin, David (1997). "The Concept of Security". *Review of International Studies* n. 23, pp. 5-26.

Nye, Joseph (2012). *TED Talks. Cyber Influence and Power*. iTunes University podcast.

Ullman, Richard (1983). "Redefining Security". *International Security* n. 1, pp. 129-153.

Wolfers, Arnold (1952). "National Security as an Ambiguous Symbol". *Political Science Quarterly* n. 4, pp. 481-502.