PRIO

PRIO POLICY BRIEF 04|2012

Cyberwar as an Issue of International law

While cyberwar is gaining recognition as a 'fifth battlefield', policy makers and the general public have insufficient knowledge about the legal and strategic implications of this development. This policy brief critically examines some of the legal and strategic challenges that arise with respect to the development of effective international and national strategies to prevent, regulate, and resolve cyberwar. To provide critical information about the role of law in the govern-ance of cyberwar, it is necessary to unpack the mutually constitutive relationship be-tween the law, empirical developments on the ground, and the cyberwar dis-course. There is a strong current push by military, political, and com-mercial actors to shift cyber security issues into the domain of warfare. The militarization of cyberspace calls for a concerted effort to promote a 'cyber peace' agenda. Moreover, while clarity about the application of the law of armed conflict (LOAC) is important, LOAC only offers a framework for addressing a small part of the cyber security challenge. More attention should be given to the lack of critical information infra-structure protection (CIIP) and the inadequate coordination of domes-tic legal regimes.

Kristin Bergtora Sandvik *Peace Research Institute Oslo (PRIO)*

Peace Research Institute Oslo (PRIO)
PO Box 9229 Grønland, NO-0134 Oslo, Norway
Visiting Address: Hausmanns gate 7

Centre for the Study of Civil War (CSCW)
PO Box 9229 Grønland, NO-0134 Oslo, Norway
Visiting Address: Hausmanns gate 7

www.prio.no
ISBN: 978-82-7288-435-1 (online); 978-82-7288-436-8 (print)

Introduction

This policy brief is funded by the Norwegian Ministry of Defense as part of a three-year post-doctoral project entitled 'Regulating Cyberwar: Understanding Challenges to Norwegian Security and International Law', aimed at surveying the multidimensional nature of cyberwar. While cyberwar is gaining recognition as a 'fifth battlefield', policy makers and the general public have insufficient knowledge about the legal and strategic implications of this development. This policy brief critically examines some of the legal and strategic challenges that arise with respect to the development of effective international and national strategies to prevent, regulate, and resolve cyberwar. To provide knowledge about the role of legislation in the governance of cyberwar, it is necessary to unpack the mutually constitutive relationship between the law, empirical developments on the ground, and the cyberwar discourse.

The concept of cyber security is the site of constant renegotiation between the domains of the market and the state, and the civil and the military. An attacker can utilize numerous computer vulnerabilities that penetrate, interfere with, disrupt, disable, steal, or destroy communications, vital information, and operating systems on numerous computer systems and networks. Methods of attack include malware containing software such as viruses, worms, logic bombs, and rootkits; zero-day threats that attempt to exploit software vulnerabilities; the use of DDoS, distributed denial of service attacks, frequently through the use of botnets; or compromising computer security through human manipulation, so-called 'social engineering'.

These threats to cyber security are commonly classified as lower-level individual crime, organized crime, cyber espionage, cyber terror, or as state-sponsored cyber attacks. Significantly, such attacks often occur in the "twilight between criminal acts and acts of war", and boundaries may be blurred between black hat hackers, patriotic hackers, and direct state participation. In recent years, cyber attacks have been recognized as a serious threat to national security, potentially amounting to acts of war. International law is considered to play a vital role in providing a framework for governing cyber attacks as threats to national and international security.

Contemporary Trends

The rise of cyberwar on the international agenda and the attendant quest for legal regulation may be explained by pointing to three contemporary trends: critical information infrastructure, such as the World Wide Web, and SCADA (supervisory control and data acquisition) systems, have become key to critical infrastructure; that is, those assets deemed central to the functioning of economy, society, and national security. As information technology hardware and software have become more technically advanced, affordable, and ingrained in daily life across the globe, a new digital landscape of citizens' activism has emerged. At the same time, the rate and severity of cyber attacks, with international organizations, governments, and corporations being attacked on a global scale, has dramatically heightened the sense of urgency at the policy level across the Western world. In response to the use of information technology in the struggle for freedom, power, or profit, governments are seeking increased control over cyberspace. Regulation is a key tool in this effort.

At the same time, the recent institutionalization of cyberwar generates a need for more legislation; a number of countries have announced that they have or plan to acquire military cyberwar units, the most well-known of which thus far is the United States Cyber Command, inaugurated in May 2010. The responsibilities and standards of these institutions must be clearly demarcated. Attendant to this, a new form cyber military-industrial complex is emerging. The continued growth of transnational IT firms such as Symantec and MacAfee is in part fuelled by the spike in cyber attacks, but also by the cyber threat assessments produced by these outfits. Traditional defense contractors, such as Northrop Grumman, Raytheon, and ManTech International now invest heavily in information security products and services. Governments need to ensure adequate regulatory supervision of this industry, and be cognizant of the keen interest the industry takes in influencing cyberwar legislation.

Cyber security is also being institutionalized at the international level. Two streams of norm-developing efforts can be discerned at the UN: an economic stream focusing on cybercrime, and a politico-military stream focusing on cyber warfare. There are strong intrastate disagreements as to how cyber attacks should be categorized (particularly between the U.S. and Russia). These disagreements also reflect part of the broader struggle concerning freedom of speech and control of the Internet. Important regional legal and policy initiatives have been initiated by ENISA (the European Network and Information Security Agency), the Shanghai Cooperation Organization (SCO), and NATO, which set up a Cooperative Cyber Defense Centre of Excellence in Tallinn in response to the 2007 cyber attacks on Estonia.

The Role of Legislation in Constituting Cyberwar

In the context of international law, there is no agreed-upon definition of cyberwar, and there is deep disagreement about when an attack might amount to an act of cyberwar: how it starts, how it ends, or how it should be conducted, as well as the potential legal ramifications. Nevertheless, a key idea underpinning contemporary cyberwar discourse is the notion of national security as being *under threat*, due to inadequate infrastructure, funding, manpower, domestic policy, and national and international legal frameworks. At the political level, whether or not an attack is classified as an economic or political-military issue by the government and the military will depend not only on the scale, sophistication, and motivation of the attack, but also on the geopolitical and strategic resources of the country under attack and the (attributed) identity of the attacker. With a burgeoning cyber lobby, there is increasingly also a commercial logic to the classification of cyber attacks as cyberwar.

Legalization provides needed legitimacy for a process of militarization. In a context where casualties have been notably absent in the two known cyberwars in Estonia and Georgia (where kinetic force produced casualties) and where the dimension of *territory* – so important for traditional legal definitions of war and battlefield – is missing, commentators have expressed doubt that 'warfare' is an adequate term to describe the consequences of cyber attacks. In this context, the framing of cyberwar as a topic for laws relevant to armed conflict and national security is prognostic; it becomes a discussion about the regulation of military solutions, and delineat-

ing the legal boundaries of the specific strategies, tactics, and objectives by which these solutions may be achieved.

Law in the Cyberwar Discourse

Cyberwar is frequently used as a metaphorical concept and the imprecise terminology for describing cyber conflict often leads to hyperbole. Because words have meaning, and metaphors matter, attention must be paid to the role of law in sustaining them. Legal discourse functions as a way of defining cyber attack as a threat to national and international security. The debate on cyberwar is dominated by three approaches.

A dominant feature of popular cyber discourse is the pervasiveness of what critical scholars have labeled 'cyber-doom scenarios' or 'cybergeddons'. Labels such as 'digital Pearl Harbor', 'cyber 9/11', 'eWMDs', or 'cyber Katharina' are also used. Cyber-doom arguments are mostly propagated by 'cyberhawks', private sector security professionals with prior security governance experience seeking contracts for equipment delivery and lucrative consultancies. In this type of imagery, Western countries and the NATO alliance are depicted as inadequately prepared for a looming cyberwar against Russia, China, North Korea, and other adversaries. Calls for the application of the law of armed conflict – or more precisely, a new and cyber-specific LOAC instrument – is frequently voiced as part of the demand for tougher government action on adversaries, more comprehensive institutionalization of cyberwar in the national security infrastructure, and more spending on both defensive and offensive cyber capabilities.

A second position rejects the militarization of cyberspace represented by the cyber doom agenda. This position argues that 'cyberwar' is not war, but in essence a computer security problem. Hence, the laws of warfare do not and should not apply.

A third, pragmatist position partially accepts the framing of certain cyber events as national security threats. It holds that regardless of labels, cyber threats are real, and that various cyber tools and techniques are becoming increasingly important in international conflict. This position focuses on the necessity of protecting critical information infrastructure. According to this perspective, resilience is the best strategy to maintain national security and avoid escalation of international cyber conflicts. Resilience is achieved by the use of both humans and technology to resist some attacks, absorb and mitigate others, and to reach out to anticipate and stop other attacks. A broad legal approach, including but not limited to the law of war, is an important component of the resilience toolbox.

An Inside View of the Evolution of Cyberwar Discourse

The evolution of the cyberwar discourse can be traced from its inception as one of several forms of information war in the early 1990s, strongly connected to the dawning of the information age and the thinking on revolution in military affairs (RMA), to its current status as a distinct form of warfare in need of legal regulation. The tension between positions arguing (a) that cyberwar represents a new type of conflict in need of new legal norms, and (b) that the existing legal framework is adequate, has been present in the cyberwar discourse almost since its beginnings. Briefly superseded by discussions on cyber terror in the aftermath of 9/11, the rise of cyberwar testifies to an ongoing militarization of cyberspace and cyber security issues.

In the struggle to develop workable norms, the absence of a commonly agreed-upon definition of cyberwar has been a problem for policy makers; definitions that are too narrow or too broad create challenges with respect to divisions of labor between civil and military domains, between the government and the private sector, and between national governments and international entities. At the same time, any such definition must be linked to a grounded understanding of the role cyber attacks may play in a conflict, from where a cyber attack serves as the enabler for kinetic force to where it amounts to an armed attack.

Current legal debate on cyberwar is dominated by three approaches: that cyberwar is difficult to regulate, that new legal instruments are needed, or that the challenge lies is applying existing norms to cyberwar in a proper manner. *The Manual on International Law Applicable to Cyber Warfare*, to be finalized in late 2012, attempts to provide a restatement of how the law of armed conflict applies to cyber conflict. The key issues under the law on the use of force and the law of war will be outlined below. It should be noted that what has been labeled 'the comprehensive legal approach' indirectly challenges the concern with war as the focal point of cyber security discourse. This approach focuses on deploying a variety of legal instruments, including the law of armed conflict, in order to combine considerations of threat, deterrence, and response from different areas of authority and responsibility.

Computer Network Attacks and the Law on the Use of Force – The Key Issues

The key issue under the jus ad bellum (law on the use of force) concerns the use of force under the Charter of the United Nations. While commentators have mostly agreed that a cyber attack may represent a prohibited use of force under article 2 (4), the threshold levels for when a cyber attack constitutes a use of force or an armed attack are still contested. Legal commentators also disagree on when a state may in engage in self-defense under article 51 in response to cyber attacks, as well as on the specific requirements for attributing responsibility for an attack to a particular nation state.

Not unique to the case of cyberwar, the interpretation of the norms of the *jus ad bellum* is generally characterized by the different strategic logics and unequal power relationships between nations. Whether political actors support strict or permissive interpretations will also depend on whether their field of responsibility is in the domain of military capabilities or in the protection of civilian infrastructure. National approaches to the use of force in cyberspace largely reflect those strategic positions generally taken on the use of force and the permissibility of self-defense in response to armed attacks.

From a doctrinal perspective, many questions remain unresolved: can the existing framework meaningfully differentiate between legal activities, such as cyber espionage, and illegal computer network attacks? What is the likelihood of reaching international consensus on the interpretation and enforcement in this area, when various types of states are likely to view cyber threats differently and to distinguish differently between what counts as offensive and defensive measures? Will some

states prefer legal ambiguity? Traditionally, treating something as an armed attack that triggers self-defense rights under article 51 has had deterrence value. As computer network attack capabilities proliferate, will a permissive authority to resort to armed force against cyber attacks introduce greater security instability to the international system by undermining constraints on military responses to non-military harm?

Computer Network Attacks and the Law of War – the Key Issues

The *jus in bello* (law of war) is the body of law concerned with what is or is not permissible during hostilities. The regulations applicable to cyber warfare are mainly found in the Additional Protocol I relating to the protection of victims of international armed conflicts from 1977 (Part V on the civilian population), and in the law of neutrality as codified in the 1907 Hague Convention. Although interpretive disagreements remain, there is general agreement among scholarly commentators as to the applicability of these norms to computer network attacks. The interpretive focus is on making distinctions between the military and civilian spheres: who is or is not protected from cyber attack, and how does a transition between the two categories occur? Who can lawfully participate in hostilities? What is or is not protected from cyber attack, and how does a transition between the two categories occur? To which means and methods must cyber attacks conform to be legal? What are the rules concerning deceit and deception applicable to cyber attacks? What respect is owed to neutral states, and what must states do to remain neutral?

The arguments concerning the thresholds for legality go to the heart of the ethics of war. While some commentators argue that a resort to cyberwar will mean more frequent targeting of civilians, others contend that rather than prevent the development of cyber weapons, the law of war should evolve to encourage states to use cyber weapons in some circumstances while also properly restraining their use in others. More broadly, the challenge for lawyers and force planners is to identify and conduct realistic exercises where relevant scenarios arise. In practice, a plethora of overlapping and competing legal regimes require states to adjust any offensive cyber-attack strategy to satisfy their obligations under various specialized regimes of international law, and to negotiate the relationship between international law obligations and domestic legal norms. However, a general problem in adapting the law of war for cyberwar is that lawyers lack the scientific and technical skills necessary to analyze technological developments. Moreover, research on cyberwar is classified and thus inaccessible.

Conclusion

Three observations are of particular relevance to policy makers:

First, while exercises of legal line-drawing are important and useful, they are also strategic and political. Many of the challenges that pertain to the understanding and conduct of cyberwar are not primarily legal in nature. There is a strong current push by military, political, and commercial actors to shift cyber security issues into the domain of warfare. Some scholars have begun to argue that cyberwar makes war more humane, and that international law should adapt to and promote cyberwar as an alternative to traditional warfare. This development may contribute to creating greater government and military control over civilian networks, leading to potential infringement on civil liberties.

Second, the focus on cyberwar as a threat to national security and international peace may misspecify the solutions to cyber security issues. While international law offers a regulatory framework for a crucial but small part of the cyber security challenge, inadequate protection of critical information infrastructure and unsatisfactory coordination of domestic legal regimes remain insufficiently addressed by policymakers in most jurisdictions. The comprehensive legal approach offers a promising way forward with its focus on legal coordination between fields such as information society and telecommunications, cybercrime, national security, and armed conflict. Advocating for this approach may also assist military leaders in demanding more proactive engagement from governments and the private sector.

Third, militarization of cyberspace calls for a concerted effort to promote a 'cyber peace' agenda. Cyber peace could be promoted by delinking cyber security issues from armed force, and by imposing a high legal threshold for treating them as equivalent. At the same time, cyber peace should not be defined only in the negative; more attention must be given to the role of international law in the development of a substantive cyber peace agenda. ■

THE AUTHOR

Kristin Bergtora Sandvik is a Senior Researcher at PRIO. Her research focuses on the interface between humanitarianism, violence and international law.

E-mail: Bergtora@prio.no

THE PROJECT

The policy brief is a deliverable from a three-year post-doctoral project, funded by the Norwegian Ministry of Defence, entitled 'Regulating Cyberwar: Understanding Challenges to Norwegian Security and International Law', aimed at surveying the multidimensional nature of cyberwar.

PRIO

The Peace Research Institute Oslo (PRIO) is a non-profit peace research institute (established in 1959) whose overarching purpose is to conduct research on the conditions for peaceful relations between states, groups and people. The institute is independent, international and interdisciplinary, and explores issues related to all facets of peace and conflict.