Technology, violence and law: Cyber attacks and uncertainty in international law

Technology, Violence and law: Cyber Attacks and Uncertainty in International law

Samuli Haataja
Griffith University, Gold Coast, Australia
s.haataja@griffith.edu.au

Abstract: In 2007 Estonia was faced with a new type of international violence that was difficult to conceptualise. Characterisations of the cyber attacks by Estonian officials at the time ranged from war, crime to terrorism. The technological makeup of cyberspace led to a range of problems for the traditional distinctions between these categories and hence international law was uncertain in its application to this new form of violence. These issues are among those generally discussed in literature on cyber attacks and international law. This literature also tends to follow a typical pattern of writing about law and technology, and arguably this does not result in a developed understanding of the relationship between law and technology. However, another body of literature exists which seeks to understand the intersection of law and technology better by looking at past events where technology created problems for the law, the socio-technical context of the law and the values that law seeks to protect. By adopting the insights from this body of literature, the uncertainties that cyber attacks (technology) creates for law will be explored. Accordingly, it will be shown that cyber attacks create a number of uncertainties for international law. On one level, this new type of violence has created uncertainties in the application of existing law and thus led to legal issues. These are centred around doctrinal issues on state responsibility (particularly attribution) and what constitutes an illegitimate use of force. On another level, they raise uncertainties about the compatibility of law premised upon a technological environment in which state sovereignty is central to regulate behaviour in an environment in which states lack a monopoly of violence and distinctions between the actors inflicting this violence is less clear. Exploring these uncertainties will lead to a more developed appreciation of how technology can shape the way we understand violence in international law.

Keywords: cyber attacks, technology, international law

1. Introduction

War, as a form of violence, has persisted throughout known history. Indeed it has been a defining feature of the modern state given the close links of notions of territory and violence to sovereignty. Besides the legal monopoly of violence afforded to states by virtue of their sovereignty, states have historically also held the exclusive technological capacity to monopolise violence. Initially this took place across land but technological advancement expanded it into the sea, air and space domains, though territory remained the physical and legal basis for sovereignty or sovereign rights within these domains. Recently however, technological change has given rise to a new form of violence complicating the traditionally held monopoly of violence by states. Cyber attacks constitute this new form of violence[1] and have become increasingly prominent in recent years. However, the prevalence of cyber attacks and the legal issues they raise has led to the general view that law is being outpaced by technology and thus unable to control this technologically enabled violence.

Using conceptualisations of the Estonia 2007 cyber attack as an example, this paper will explore why and how technology (cyber attacks) has resulted in this perception that law is falling behind technological developments. In doing so it will also explore the broader uncertainties that cyber attacks raise for international law. The first part of this paper will outline the different conceptualisations of the cyber attacks evident in Estonia's official responses to the attacks. It will also provide a brief account of how existing literature tends to differentiate these conceptualisations (war, crime and terrorism) and how these become problematic in the cyber context. The second part will review how existing literature on cyber attacks and international law tends to characterise the problems that technology creates for law and how the approach of this literature to the relationship between law and technology is rather narrow. It will also outline existing literature that seeks to provide more sophisticated understandings of the relationship between law and technology. Part three will then discuss the uncertainties in international law made evident by the new form of violence that cyber attacks embody. Collectively this paper will demonstrate that a broader understanding of the relationship between law and technology is needed in order to fully appreciate the uncertainties that

[1] For the purposes of this paper, the notion of violence is used to avoid context specific distinctions between different types of 'armed conflicts' and those that do not fit within these legal constructs. The term 'cyber attack' is also used broadly as a means of distinguishing this novel form of violence from the traditional types of violence that international law has been concerned with.

cyber attacks raise for international law and how technology can shape the way we understand violence in international law.

2. Estonia 2007

In 2007 Estonia was subject to a new type of violence which was vectored through cyberspace. Estonia was victim to a number of waves of cyber attacks following its government's decision to relocate a politically contentious war memorial statue.[2] Given the scale and duration of these attacks against a state heavily reliant on the internet, the events were widely described in the media as a cyber war (Landler and Markoff, 2007)(Farivar, 2007). The Estonian government's initial responses in early May reflected the rhetoric, as it was believed that the cyber attacks were part of a broader Russian attack against Estonia and hence that Estonia was under attack from Russia (Paet, 2007a)(Ansip, 2007).[3]

In the days and months that followed the attacks, Estonian officials described the cyber attacks as a part of a war, as crime and as terrorism. On 1 May, Estonia's Minister of Foreign Affairs declared that '[t]he European Union is under attack, as Russia is attacking Estonia' (Paet, 2007a). This was echoed the following day in a speech by the Prime Minister to the Riigikogu (the Estonian Parliament), who stated that the sovereign state of Estonia was 'under a heavy attack' (Ansip, 2007). On the other hand, on 11 May the Minister of Foreign Affairs spoke at a Council of Europe committee meeting about the ongoing incident, however he framed this within the language of cyber crime and the Convention on Cybercrime framework urging Russia to take measures against cyber criminals operating within its territory (Paet, 2007b). In the lead up to a meeting of European Union defence ministers on 14 May, Estonia's Minister of Defence made a statement raising issues regarding whether cyber attacks could constitute military action under the North Atlantic Treaty Organisation framework, thus allowing for the invocation of the North Atlantic Treaty's collective security provisions (Estonian Ministry of Defence, 2007). In this context, he stated that 'not a single NATO defence minister would define a cyber attack as a clear military action at present; however, this matter needs to be resolved in the near future' (ibid). A day after the meeting, the Estonian Minister of Defence compared the attacks to terrorism stating that, given the 'scale of damage and the way these cyber-attacks have been organised, we can compare them to terrorist activities' (AFP, 2007). Additionally, the following month the Minister of Defence explicitly identified the problem of classification stating that '[i]n our minds, what took place was cyber-warfare and cyber-terrorism' (Aaviksoo, 2007).

In November 2007, approximately six months after the attacks, Estonia's Minister of Defence gave a speech in which he backed away from describing the events as 'cyber war' stating that the term had 'no real content for the time being' (Aaviksoo, 2007). Instead, he said he 'tend[s] to term the events that took place in Estonia … as cyber-terrorism' (ibid). This is largely reflected in the impact and objectives of the attacks, described by the Minister of Defence to have been primarily of 'psychological nature' causing intimidation of the people and limiting their access to information online (ibid). However, despite the lack of long term consequences or physical harm or destruction caused by the attacks, they were nonetheless stated to have 'posed a serious threat to Estonian sovereignty' (ibid).[4]

The three different classifications of the cyber attacks evident in these responses show at least three legal regimes that are potentially applicable. These range from the general 'use of force' regime, the international laws seeking to tackle cyber crime and the international prohibition on terrorism. This also results in three different (though sometimes overlapping) conceptualisations of who was responsible for the attacks and what the legal and practical implications of that responsibility mean. If regarded as cyber war then Russia would have been the enemy creating the threat. If classified as cyber crime or terrorism, then cooperation would have been sought with Russia to end the attacks launched by the culprits. Thus the responses to the cyber attacks were mixed and the implications of each different characterisation varied in seriousness and in terms of who was responsible for the threat. As will be shown, this was a result of uncertainties in international law (especially at the time) about how to classify such an attack. Nonetheless, as the Minister of Defence's speech in November 2007 demonstrated, even six months after the attacks Estonia continued to believe that its sovereignty was threatened by this new form of violence and there remained uncertainty about how to

[2] For a detailed account of the events, see (Tikk, Kaska and Vihul, 2010).

[3] Despite the lack of concrete evidence to prove or disprove who was responsible for the attacks, some regard a degree of Russian government involvement as the only plausible explanation (Ottis, 2008).

[4] Domestically however, the attacks were treated as criminal acts (Czosseck, Ottis and Talihärm, 2011).

conceptualise it under international law. As the following sections will demonstrate, much of this uncertainty in how to conceptualise the attacks was a result of perceived 'gaps' in the international legal framework at the time dealing with cyber attacks.

The uncertainties faced by Estonia in conceptualising the cyber attack are also the focus of much of the literature on cyber attacks and international law. As demonstrated by Estonia's official responses, cyber attacks can be classified as war, crime or terrorism and hence can fall under different legal regimes. A common way this classification is made is by looking at the intention and/or identity of the actors involved. Shackelford for example notes the difficulty of discovering the identity of those responsible for cyber attacks due to the speed of attacks and the attackers' ability to maintain their anonymity (Shackelford, 2009, p. 232) This problem is exacerbated by the fact that boundaries between crime and terrorism are breaking down more generally, and in cyberspace states can encourage private actors to commit cyber attacks and hide behind a veil of plausible deniability (ibid, p. 233). Hollis makes a similar point, noting that the current architecture of the internet makes it 'difficult to know which set of proscriptions—crime, war, or terrorism—applies' (Hollis, 2011, p. 378) to a cyber attack.

Indeed, even in the real world there are problems with classifying an act into these categorises, because, according to Osler, '[t]he system breaks down when acts of crime look like war, and acts of war look like crime'(Osler, 2003, p. 604). Brenner highlights the added difficulties of making these distinctions in cyberspace, noting that 'these threat dichotomies break down when attacks are vectored through the virtual world of cyberspace' (Brenner, 2009, p. 70). Thus, as will be demonstrated, technological change is further complicating these distinctions between different types of violence (be they traditionally characterised as war, crime or terrorism), highlighting challenges to existing law and leading to the view that law is being outpaced by technology.

3. Existing literature

Besides discussing the need to determine an actor's identity and intentions in order to classify a cyber attack, existing literature on cyber attacks and international law also tends to follow a similar pattern of writing about the relationship between law and technology. In fact, this pattern of writing is not unusual for people writing about legal problems created by technology. This pattern is described by Tranter as the 'law and technology enterprise' (Tranter, 2011) and usually begins with a technological crisis or event that reveals gaps in the law or creates challenges to existing law (ibid, p. 32). It then moves on to describe new, generally value-free law which is needed to fill these gaps. Given a positivistic approach to the law, the values that law embodies are not debated and law is simply reduced to a means of implementing policy (ibid, p. 70). Further, the historical relationship between developments in technology and law is often neglected (ibid, p. 72). Effectively this narrows the ways in which the relationship between law and technology is explored and it is also assumed that law has the capability to 'control the impacts of technological change' (ibid, p. 70).

The literature on cyber attacks and international law largely follows this pattern of writing about law and technology. A technological crisis or event is identified (the attacks against Estonia are commonly used as an example) or the destructive potential of cyber attacks is emphasised. For example Hollis notes the 'enormity of the cyberthreat problem' (Hollis, 2011, p. 390) and that '[i]n terms of effects, cyberthreats can be merely annoying or apocalyptic' (ibid). Similarly Shackelford maintains that 'cyber attacks represent a threat to international peace and security that is potentially as daunting and horrific as nuclear war' (Shackelford, 2009, p. 198). The picture painted is mostly grim as cyber attacks can have unfathomable and apocalyptic consequences, and in scale can be comparable to nuclear attacks. This crisis event then reveals or highlights 'gaps' in the law as it is unable to 'keep up' with technology. For example Hathaway et. al. argue that '[c]yber-attacks present a new and growing threat—one that current international and domestic laws are not yet fully prepared to meet' (Hathaway et al, 2012, p. 877) and that new international law is needed to 'fill the gaps in existing law' (ibid). Even the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013) expressly acknowledges that given the speed of development of these technologies, 'cyber practice may quickly outdistance agreed understandings as to its governing legal regime' (Schmitt, 2013, p. 3).

This literature also presents a common solution to addressing the problems. The solution is the creation of new law designed specifically for cyber attacks or one that extends existing law to this technology (Hathaway et al, 2012)(Hollis, 2011)(Hoisington, 2009, p. 441)(Shackelford, 2009, pp. 197-198). Finally, the literature tends

to focus on the applicability of international legal doctrine to cyber attacks and consequently provides a rather positivistic account of law. Specifically, the law on the use of force (*jus ad bellum*) and law in war (*jus in bello*) are common areas of international law discussed by authors engaging in debates about whether, how and why these bodies of law can be extended to cyber attacks (Waxman, 2011)(Schmitt, 1998-1999)(Schmitt, 2012)(Jensen, 2002)(Hoisington, 2009)(Brown, 2006)(Hollis, 2007)(Shackelford, 2009)(Hathaway et al, 2012).

Therefore this literature generally regards cyber attacks as a novel technological development creating new challenges to international law. The way to respond to these challenges is the creation of new law. However, the approach towards law is primarily positivistic, as the focus of much of this literature is on international legal doctrine with the political, social and technological context of law left marginalised. Despite some exceptions, this is largely the pattern of writing about law and technology that the cyber attacks and international law literature reflects. This is ultimately a narrow way of understanding the relationship between law and technology ignoring the historical relationship between the two, the technological environment in which law operates and the values that the law seeks to protect.

4. Law and technology

Another body of scholarship that focuses on law and technology more broadly seeks to address these concerns. Scholars within this body of literature seek to provide a more sophisticated understanding of the relationship between law and technology. They recognise that law and technology issues are not new and acknowledge other (now) historical events in which the two have intersected. They also consider the values that law protects and the socio-technological environment in which the law exists in order to provide a more fruitful account of the relationship between law and technology (Tranter, 2011, pp. 72-73). For example Mandel looks at the 'lessons that can be learned from past responses to once-new legal issues created by technological advance' (Mandel, 2007, p. 552) which help to understand the 'current and future law and technology issues' (ibid) that arise. Cockfield in turn argues that 'technological developments can undermine important interests and values that the law seeks to protect' (Cockfield, 2003-2004, p. 338) and that one needs to consider the 'broader context of technological changes that may affect important interests and values' (ibid, p 384). Gifford seeks to address the ways in which law and technology interact, one being 'when society decides that technology produces undesirable results and employs legal rules to contain or modify those results' (Gifford, 2007, p. 572). Therefore these authors stress the importance of history, the values that law protects and understanding the socio-technological environment in which law exists in order to better understand the relationship between law and technology.

Bennett Moses is another prominent 'law and technology' scholar who notes that the relationship between law and technology is often described as a race, with law always falling behind the pace of technology (Bennett Moses, 2007a). However, she seeks to provide a more detailed account of why and under what conditions law is outpaced by technology, in order to better understand the relationship between the two. According to Bennett Moses, technological change is change in what actors are practically or 'technically capable of doing' (Bennett Moses, 2007b, p. 598). This occurs when new forms of conduct are made possible that adjusts the limitations placed on actors by the previous technological state of affairs (Bennett Moses, 2007b, p. 594). Sometimes this leads to moments in time that the law has problems in dealing with this new form of conduct revealing 'gaps' in the law (Bennett Moses, 2007a, p. 241). Additionally, technological change can reveal the socio-technical context that previously underpinned the law. A situation in which 'gaps' in the law may be revealed occurs when law is uncertain in its applicability to new forms of conduct made possible by technological change (Bennett Moses, 2007a, p. 248).

While a degree of legal uncertainty can exist prior to technological change, this uncertainty tends to be amplified by technological change (ibid, pp. 250-253). Whether a new form of conduct is permissible or not will depend on whether it fits into an existing legal category. However, some forms of new conduct made possible by technological change cannot be easily classified as they do not fit easily into the existing legal categories (ibid, pp. 235-255). At other times, the issue is not with the new form of conduct, but instead with the legal category itself as '[s]ome legal categories and concepts become ambiguous in light of technological change' (ibid, p. 257). Thus these uncertainties that result from technological change are unique and more problematic than simply legal uncertainty as they arise from the technology itself (ibid, p. 257-258).

5. Cyber attacks and uncertainty in international law

Uncertainty is a particularly prominent reason for why legal issues are raised by cyber attacks and the 'technological change' that they embody. While there is no specific point in time at which cyberspace technologies 'changed' and led to legal problems, the wide scale cyber attacks in 2007 against a state so reliant on the internet marked a significant event that led to increased discourse about these issues. The new forms of conduct made possible, as reflected by the Estonia incident included: the ability of non-state actors to exploit legitimate internet technologies and protocols and launch large scale cyber attacks against a state; the potential of governments to support such actors while maintaining plausible deniability and avoiding existing international legal obligations; the ability to undermine a state's sovereignty in its cyberspace in previously inconceivable ways (especially given the increasing reliance of states on the internet); and the ability of actors to do this with relative anonymity. Thus broadly, the technological change resulted in a wider range of actors (including those whose identity remains unknown) with the ability to engage in a unique type of violence in cyberspace. As the abovementioned literature on cyber attacks and international law demonstrates, the technological change that cyber attacks embody have led to challenges for the law or revealed 'gaps' in the law. Here the law and technology literature, specifically the writings of Bennett Moses, helps us understand why these problems arise.

As demonstrated by Estonia's mixed responses to the cyber attacks, it was faced with a number of uncertainties at the time. These uncertainties were largely doctrinal uncertainties. They revolve around questions of attributing state responsibility and whether a cyber attack can constitute a use of force. While there existed a degree of legal uncertainty in both of these contexts, these uncertainties were amplified by technological change. Instead of physical acts of violence committed by clearly identifiable actors, the attacks Estonia faced were vectored through cyberspace and were difficult to successfully trace due to technological structure of the internet and use of attacks that exploited this structure. Further, as a kind of violence in cyberspace, the cyber attacks also highlighted the uncertainty in the 'use of force' as a concept and whether it could include non-traditional uses of force made possible by technological change.

However, the uncertainties that this new form of technologically enabled violence creates are not limited to legal doctrine, which is largely the focus of existing literature on cyber attacks and international law. Instead, there is also uncertainty on another level about the compatibility of law, premised on the monopoly of violence of states, to regulate behaviour in a different technological environment. Historically, international law was concerned with ways in which to protect a state's sovereignty over its territory and developed throughout a time when the nature of violence was primarily physical and the primary actors were states. Further, the technological ability to engage in large scale violence (war) was regarded as solely within the realm of states and at times this ability was regarded as a defining feature of sovereignty. Only states held this right and technological capacity and international law on the use of force was developed by states around this technological context. International law's history with the regulation of violence has also been mixed, though state sovereignty and their consequent monopoly of violence have remained central in this history. While changing over time, the overriding purpose of the *jus ad bellum* for example was to provide restrictions and prescriptions on the violent conduct of states. However, these rules were developed over time to deal with different forms of physical violence by one state that threatened the sovereignty of another state. In this regard, international law was built around a certain technological environment – one in which states were the only actors who held this ability to engage in wide scale violence, both legally and practically (or technologically).

Due to technological change, there has been a diffusion of power in cyberspace and states are no longer able to maintain a monopoly of violence in this realm. Thus power relationships are changing, though international law remains premised on a different technological environment in which state power is supreme. As the technological change reflected in the Estonia incident demonstrates, a new technological environment has been made apparent in which states are no longer the sole actors capable of engaging in an effective form of wide scale violence. Nor is it always clear when a state is involved in acts of violence as the current technological environment makes it easy to mask one's identity and thus blurs traditional legal distinctions of acts for which states may be responsible for. Consequently, there is not just uncertainty about how existing legal doctrine on state responsibility should apply or what legal regime cyber attacks should be categorised into. There is also uncertainty as to the ability of international law, structured around the centrality of sovereign states and based on the assumption that states are the only actors technologically capable of

maintaining a monopoly of violence, to regulate behaviour in cyberspace where power is more diffused, violence is no longer solely physical, distinctions between violence inflicted by state and non-state actors is less clear, and physical territory is less fundamental. This raises questions about the significance of territoriality, physicality and violence to sovereignty and international law, and reinvigorates one of the central concerns of international law – its ability to control international violence.

6. Conclusion

Collectively, this paper has sought to demonstrate how cyber attacks, as a new form of violence made possible by technological change, create uncertainties for international law leading to the belief that law is being outpaced by technological change. While the traditional conception of international law is inherently state based with a close connection to physicality and territoriality, the current technological environment is characterised by different power structures. Cyber attacks represent technological change reflective of this new technological environment, hence challenging some of these traditional assumptions. However, these uncertainties are not limited to legal doctrine as is the focus of much of existing literature and instead raise more fundamental questions about the relationship between technology, violence and international law. This paper has shown that a broader account of the relationship between law and technology is needed to better understand how technology shapes our understandings of violence in international law. This in turn will help us obtain a better understanding about how and why international law is being outpaced by technological change, an understanding of the past and present technological environment of international law and how technology can shape the way we understand violence in international law.

References

Aaviksoo, J. (2007) "Cyber-Defense: Estonia's Recent Experience of this Unnoticed Third World War", Paper presented at 24th International Workshop on Global Security, Paris, http://www.csdr.org/2007book/aaviksoo07.htm.

AFP. (2007) "Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks", *The Sydney Morning Herald* [online], 17 May, http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html.

Ansip, A. (2007) "Prime Minister Andrus Ansip's speech in Riigikogu", [Press Release], 2 May, http://valitsus.ee/et/uudised/pressiteated/majandus-ja-kommunikatsiooniministeerium/13183.

Bennett Moses, L. (2007a) "Recurring Dilemmas: The Law's Race to Keep Up with Technological Change", *University of Illinois Journal of Law, Technology & Policy,* Spring, No. 1, pp 239-286.

Bennett Moses, L. (2007b) "Why Have a Theory of Law and Technological Change?", *Minnesota Journal of Law, Science & Technology*, Vol 8, No. 2, pp 589-606.

Brenner, S. W. (2009) *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford University Press, New York.

Brown, D. (2006) "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal,* Vol 47, No. 1, pp 179-221.

Cockfield, A. J. (2003-2004) "Towards a Law and Technology Theory", *Manitoba Law Journal*, Vol 30, No. 3, pp 383-416.

Czosseck, C., Ottis, R. and Talihärm, A. M., (2011) "Estonia after the 2007 Cyber Attacks", *International Journal of Cyber Warfare and Terrorism*, Vol 1, No. 1, pp 24-34.

Estonian Ministry of Defence. (2007) "Minister to attend meeting of EU defence ministers in Brussels", [Press Release], 13 May, http://www.kmin.ee/en/1429.

Farivar, C. (2007) "Cyberwar I", *Slate* [online], 22 May, http://www.slate.com/articles/technology/technology/2007/05/cyberwar_i.html.

Gifford, D. J. (2007) "Law and Technology: Interactions and Relationships", *Minnesota Journal of Law, Science & Technology*, Vol 8, No. 2, pp 561-588.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012) "The Law of Cyber-Attack", *California Law Review*, Vol 100, No. 4, pp 817-886.

Hoisington, M. (2009) "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International & Comparative Law Review*, Vol 32, No. 2, pp 439-454.

Hollis, D. B. (2007) "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review*, Vol 11, No. 4, pp 1023-1062.

Hollis, D. B. (2011) "An e-SOS for Cyberspace", *Harvard International Law Journal*, Vol 52, No. 2, pp 373-432.

Jensen, T. E. (2002) "Computer Attack on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense", *Stanford Journal of International Law*, Vol 38, No. 2, pp 207-240.

Landler, M. and Markoff J. (2007) "After Computer Siege in Estonia, War Fears Turn to Cyberspace", *The New York Times*, 29 May.

Mandel, G. N. (2007) "History Lessons for a General Theory of Law and Technology", *Minnesota Journal of Law, Science & Technology*, Vol 8, No. 2, pp 551-570.

Osler, M. (2003) "Capone and bin Laden: The Failure of Government at the Cusp of War and Crime", *Baylor Law Review*, Vol 55, No. 2, pp 603-616.

Ottis, R. (2008) "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" in Remenyi D. (ed) *Proceedings of the 7th European Conference on Information Warfare and Security*, Academic Publishing Limited, Reading.

Paet, U. (2007a) "Declaration of the Minister of Foreign Affairs of the Republic of Estonia. E. Government", [Press Release], 1 May, http://valitsus.ee/et/uudised/pressiteated/majandus-ja-kommunikatsiooniministeerium/13634.

Paet, U. (2007b) "Address by Minister of Foreign Affairs of Estonia Urmas Paet", [Press Release], 11 May, http://www.vm.ee/?q=en/node/3665.

Schmitt, M. N. (1998-1999) "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law*, Vol 37, No. 3, pp 885-938.

Schmitt, M. N. (2012) "Classification of Cyber Conflict", *Journal of Conflict & Security Law*, Vol 17, No. 2, pp 245-260.

Schmitt, M. N. (ed) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge.

Shackelford, S. J. (2009) "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" *Berkeley Journal of International Law*, Vol 27, No. 1, pp 192-252.

Tikk, E., Kaska, K. and Vihul, L. (2010) *International Cyber Incidents: Legal Considerations,* Coperative Cyber Defence Centre of Excellence, Tallinn.

Tranter, K. (2011) "The Law and Technology Enterprise: Uncovering the Template to Legal Scholarship on Technology", *Law, Innovation and Technology*, Vol 3, No. 1, pp 31-83.

Waxman, M. C. (2011) "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law*, Vol 36, No. 1, pp. 421-459.

versity, Taiwan in 1997, and both a M.Sc. degree and a Ph.D. (Computer Science and Engineering) from National Sun Yat-sen University, Taiwan in 1999 and 2010, respectively. His research interests include Internet security, wireless network, home network system, IoT, and learning cloud services.

Eric Filiol is the head of the Operational Cryptology and Virology at ESIEA. He has spent 21 years in the French Army. He holds an Engineer diploma in Cryptology, a PhD and a Habilitation Thesis in applied mathematics and computer science. He is also the Scientific Director of EICAR and the Editor-in-chief of the Journal in Computer Virology.

Jason Flood, MSc is currently an Ethical Hacking Architect at IBM in Dublin. He is also a PhD student at the Institute of Technology Blanchardstown where he investigates better ways of training Network Administrators. Jason is the co-founder Irish Chapter of the Honeynet Project and works with OWASP and Facebook in running CTF competitions.

Grigorios Fragkos, BSc, MSc, PhD, Certified TigerScheme, AST and QSTM. He has a number of publications in Computer Security and Computer Forensics. He has been part of the CyberDefense dept. of the Hellenic Army acting as Information Security consultant and Penetration tester. Currently, works for Sysnet Global **Solutions as Sr. Consultant and Penetration tester.**

Wendy Goucher is about to enter the final phase of her PhD research. She is a part time student at University of Glasgow and is also an information security consultant with Idrach Ltd. where she specialises in assisting in the design and communication of operationally effective security policy.

Dijana Grd comes from Croatia. She is a second year student of graduate study programme Information and Software Engineering at Faculty of Organization and Informatics in Varazdin. Her studies have provided her an insight into area of identification, collection, processing, analysis and production of electronically stored information. She has some work experience as a student assistant in Informatics and as a project manager in student organization AIESEC. She enjoys participating in all kind of international conferences and projects. She also likes to travel and meet new people.

Clement Guitton is a PhD candidate in War Studies at King's College London focusing on cyber security. He holds a master degree both in international relations and in electrical engineering. Fluent in English, French, and German, he previously worked at the International Telecommunication Union, the United Nation agency specialised on information and communication technologies.

Håkan Gunneriusson has a PhD in History 2002, Uppsala University. Hakan is interested in sociological and historical perspectives on current and coming issues regarding military tactical and cultural issues. Hakan is currently head of research ground operative and tactical areas, Swedish National Defence College.

Samuli Haataja is a PhD candidate in the Griffith Law School at Griffith University on the Gold Coast, Australia. He holds a Bachelor of Laws (Hons) and Bachelor of International Relations from Griffith University. His research focuses on cyber attacks and international law – specifically on the relationship of technology, violence and law in this context.

Mikko Hakuli is currently employed as security specialist at JyvSecTec-project in Jyväskylä University of Applied Sciences (JAMK), where his main responsible are technical security testing and development of various situational awareness "best practices" in cyber-security area. Formerly he worked as Head of information security on Finnish Airforces. Currently he also make studies in University of Jyväskylä and Jyväskylä University of Applied Sciences.

Juhani Hämäläinen received his PhD degree in theoretical physics from the University of Jyväskylä in 2004. He is currently in the position of principal scientist at Finnish Defense Forces Technical Research Centre (PVTT). His research interests include mathematical model development and operational analysis.

Major Arto Hirvelä is an instructor (leadership) in a research group at the Finnish National Defence University. He is preparing a doctoral dissertation in Military Science (leadership). His research interests are information environment, strategic communication, and information operations.

Ilona Ilvonen is a doctoral student at Tampere University of Technology, department of Information Management and Logistics. Her doctoral thesis topic is the management of knowledge security, and the thesis is due in 2013. She has published conference papers on information security management, knowledge management and relating topics since the year 2003.

Margarita Jaitner is a research intern at the Finnish National Defence University. She received a Bachelor's degree in Political Science at the Swedish Defence College and is currently pursuing a Master's degree in Societal Risk Management at the Karlstad University in Sweden.