Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM

Scott J. SHACKELFORD[a,1]

[a]*University of Cambridge, Cambridge, UK*

Abstract: This Article reviews both the applicability and desirability of the two vying regimes for state responsibility under international law as applied to cyber attacks: the effective and overall control standards. Due to the technical difficulties with proving attribution for cyber attacks, along with the unreasonably high burden of proof required by the ICJ's interpretation of the effective control standard, this Article argues for the adoption of the overall control standard as being both within the best interests of NATO as well as the international community.

Keywords: state responsibility, cyber attacks, international law, NATO, cyber security

1 Department of Politics and International Studies, University of Cambridge, 17 Mill Lane, Cambridge, CB2 1RX, UNITED KINGDOM, Email: ss645@cam.ac.uk.

INTRODUCTION

At a time in which the unchecked sovereign authority of States is being challenged across many arenas, State responsibility remains a key bulwark of international security (Held, 2006, p. 293-97; Reich, 1991). But constructing a viable regime to define State responsibility in international law has proven to be elusive. Instances of State-sponsored terrorist acts have increased since the end of the Cold War, but proving State responsibility for such acts remains exceedingly difficult (Brenner & Crescenzi, 2006, p. 398; Burgess 2006, p. 302; Joyner & Rothbaum, 1993, p. 229). This problem is magnified in cyberspace by the speed and anonymity of cyber attacks, making according to the White House "distinguishing among the actions of terrorists, criminals, and nation States difficult." (*National Strategy to Secure Cyberspace,* 2003, p. 19 & p. 64). As seen in the 2007 cyber attack on Estonia, a potential sponsoring State may not cooperate in the investigation, apprehension, and extradition of those who committed criminal or terrorist acts on its behalf (Davis, 2007). Given the clandestine nature of cyberspace, States may thus incite civilian groups within their borders to commit cyber attacks and then hide behind a, however sheer, veil of plausible deniability and thus escape accountability.

This Article analyzes the two primary legal regimes of State responsibility for cyber attacks that could mitigate such State sponsorship: the effective and overall control standards. In brief, the effective control doctrine, originating in the International Court of Justice (ICJ) *Nicaragua* case, recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State (Nicaragua v. United States, 1986, p. 110). In contrast, the overall control doctrine, illustrated in the International Criminal Tribunal for the Former Yugoslavia *Tadic* case, held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control such that the group's acts are attributable to the State (Prosecutor v. Tadic, 1995). This Article argues for the adoption of the latter standard of State responsibility for cyber attacks given the extreme technical difficulties involved with proving the identity of cyber attackers.

The Article is structured as follows. Part I constitutes a brief literature review on the question of appropriate standards of State responsibility for cyber attacks, taking special note of the unique scholarly contribution of this Article. Part II summarizes some of the myriad technical challenges raised by tracing cyber attacks. Part III discusses the fundamental problem of attribution as well as the cases for and against the effective and overall control standards of State responsibility for cyber attacks. Finally, Part IV demonstrates how defining State responsibility is critical within the context of NATO's cyber security strategy.

1. LITERATURE REVIEW HIGHLIGHTING ORIGINAL CONTRIBUTION

The literature to date has only obliquely dealt with the issue of State responsibility for cyber attacks in international law. Some works note that armed coercion is generally chargeable to States more so than other forms of coercion, but do not address the degree of proof needed to constitute State responsibility (Schmitt, 1998, p. 885). Other articles adopt *Nicaragua's* framework as applied to non-State actors, but not necessarily States (Schapp, 2009, p. 145). Much of the rest of the existing scholarship focuses on cyber terrorism by non-State actors, such as Verton (2003) or Ryan (2007). The one recent collection of essays on cyber warfare entirely ignores the topics of State responsibility, attribution, sovereignty and management of the information commons, all of which are central to countering cyber attacks (Janczewski & Colarik, 2008). There is thus a paucity of literature dealing with cyber attacks from the lens of international law and relations, to say nothing of the ethical and human rights implications of cyber attacks on national and international security (Wolf, 2000, p. 95; Yang, 2006, p. 201). Treatments of cyber attacks and information warfare outside the orthodox international humanitarian law framework are also nearly non-existent (Hanseman, 1997, p. 173). In particular, the literature to date has been silent on the appropriate legal regime to use as a baseline for regulatory responses to cyber attacks despite the fact that a developed system of treaties on the law of war now governs many aspects of the conduct of modern warfare, from weapons of mass destruction to the treatment of POWs and non-combatants.[2]

Nor has the growing literature on the rise of Internet law and the information commons applied its findings to the question of State responsibility for cyber attacks (Hunter, 2003; Johnson & Post, 1996, p. 1367; Lessig, 1999, p. 500). Even those recent works that do address cyber attacks and critical infrastructure protection do so primarily from a U.S.-centric vantage point, such as Cordesman (2002), or Lulasik (2003). Consequently, there is an important gap in the international law literature that this work addresses by explicitly laying out the cases for and against each potential regime of State responsibility for cyber attacks, analyzing the relative strengths and weaknesses in the context of NATO operations, and making a case for the adoption of the overall control standard. Before the respective options for State responsibility are examined though, first a brief introduction of the technical challenges of tracking cyber attacks is warranted.

---

2 The United States, for example, is party to eighteen law-of-war treaties. For a survey, see U.S. Department of State, Treaties in Force, 2007, *available at:* http://www.state.gov/s/l/treaty/treaties/2007/index.htm.

2. A BRIEF SUMMARY OF THE SCIENCE OF TRACING CYBER ATTACKS

The science of tracing cyber attacks is primitive at best. Sophisticated attacks by knowledgeable hackers, whether private or State-sponsored, are nearly impossible to trace to their source using modern practices (Lipson, 2002). The current foundation of network communications in cyberspace, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), dates back to 1982 (Lipson, 2002, p. 5). It is this antiquated system of communication designed for a small number of academic and governmental researchers sharing information with low risks of system breaches, which is at the heart of the problem for tracing cyber attacks (Lipson, 2002, p. 14). Though, of course, this is not the only problem—system vulnerabilities are multiplied when considering the myriad problems with often rushed to market commercial off-the-shelf software. Other issues include the facts that: the Internet was never designed to track or trace users, or to resist untrustworthy users; a packet's source address itself is untrustworthy and is easily masked; the current threat environment in cyberspace exceeds the Internet's design parameters; and there are myriad strategies that hackers employ making tracking difficult, such as tunneling and the destruction of data logs. But the overarching issue is that the current system was designed for a small number of trustworthy and tech-savvy researchers, which is simply no longer the case with more than a billion Internet users worldwide (Internet: *General Usage Statistics,* 2003).

Can the cyber infrastructure be modernized to enhance security and stop cyber attacks once and for all? The short answer is yes, but not easily. Certain strategies pioneered by the U.S. Cyber Emergency Response Team (USCERT) are promising, such as the use of probabilistic traceback techniques to audit a small percentage of packets so as to find the source of major distributed denial-of-service (DDoS) attacks of the kind that Estonia suffered in March 2007 (Hughes, 2009). There is also the possibility of tracing back single IP packets, though this is much more difficult (Lipson, 2002, p. 27). A full review of the myriad technical issues and their potential solutions is beyond the scope of this Article. Suffice it to say though, ultimately these technical countermeasures will never offer a complete solution to the problem of cyber attacks. Cyberwarfare is an arms race that cannot be won by defense alone. In the end, these attacks will likely continue to proliferate both in numbers and severity; the question then is how best they should be dealt with in international law and relations.

3. THE FUNDAMENTAL ISSUE OF ATTRIBUTION AND THE CASE FOR THE OVERALL CONTROL STANDARD

Attribution of a cyber attack to a State is a, if not *the*, key element in building a functioning legal regime to mitigate these attacks. The laws of war requires one State to identify itself when attacking another State, though this convention is honored more in the breach than in compliance (Brenner, 2006, p. 398; *The Hague Convention Relative to the Opening of Hostilities*, 1910, art. I). When there is a question about State sponsorship of aggression, two competing standards for State responsibility now exist in international law under Article VIII of the International Law Commission's Draft Articles on the Responsibility of States for International Wrongful Acts. Article VIII implicates State control when State actors or official organs are acting under the direction of the State (*Responsibility of States for Internationally Wrongful Acts*, 2001). An exact definition of 'control,' however, has been left up to the courts to interpret. The first standard that the courts have created is the ICJ *Nicaragua* effective 'operational control' standard (Nicaragua v. United States, 1986, p. 392). *Nicaragua* requires that a country's control over paramilitaries or other non-State actors can only be established if the actors in questions act in "complete dependence" on the State. The second standard is the ICTY *Tadic* 'overall control' standard. The ICTY held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control, and the group's acts are attributable to the State (Prosecutor v. Tadic, 1995, para. 70). In so finding, the majority interpreted the decision of the ICJ in *Nicaragua* as requiring the government of a State to exercise "effective" control over the operations of a military force in order for the acts of that force to be imputed to the State (Pronk, 1997).

The most recent case in which the ICJ reviewed the competing standards of State responsibility was the *Application of the Genocide Convention ("Bosnian Genocide").* There, the Court adopted the effective control rather than the overall control standard in deciding that Bosnia lacked the specific intent to commit genocide (Bosnia and Herzegovina v. Serbia and Montenegro, 2007; Cassese, 2007). In essence, the Court required "smoking-gun" evidence or its equivalent (Luban, 2007, p. 30). The standard laid down by the Court was beyond *any* doubt, not beyond a *reasonable* doubt. This distinction is significant enough to potentially have been dispositive of the case's outcome, just as it is for holding State sponsors of cyber attacks accountable. Future cases will also likely turn on this distinction, necessitating an in depth analysis of the benefits and drawbacks of each standard for State responsibility.

3.1 THE CASE AGAINST THE EFFECTIVE CONTROL STANDARD

As a result of the divergence in international law on the issue of State responsibility, there are two competing standards emerging for cyber attacks: the effective control standard applicable to non-State actors, and both the effective and overall control standards applicable to State sponsors of cyber attacks. For non-State actors, the ICJ held in *Nicaragua* that effective control was the appropriate standard to apply at least in the paramilitary context of that case (Capaldo, 2007, p. 104). If this decision were to be extended to cyber militia, it would mean that the only instance in which State sponsors of cyber attacks would be held accountable for their involvement would be if their effective control could be proven beyond *any* doubt. Given what has been demonstrated about the extreme technical difficulties of proving the identity of cyber attacks due to the nature of the Web's architecture, such a standard would in essence give a free pass to State sponsors of cyber attacks. In a sophisticated global cyber attack, missing or corrupted data commands may be sufficient to disprove State control and defeat accountability. Without either new techniques such as the probabilistic tracing project mentioned in Part II, or very unsophisticated hackers, effective control would make State responsibility for cyber attacks virtually a non-starter.

There are other important drawbacks to adopting the ICJ's *Nicaragua* formulation with regards to proving State responsibility for cyber attacks, among them being the fact that the Court divided the use of force into "most grave" and "less grave" categories (Nicaragua v. United States, 1986, p. 101). This distinction has split commentators. Some see this view as formalistic and restrictive, and according to Gray (2000, p. 141) it "will encourage aggression of a low-key kind." Others see a low threshold of armed attack mixed with collective self-defense as a recipe for the internationalization of civil conflicts (Watkin, 2004, p. 5). As applied to cyber attacks, this doctrine could arguably give low-level cyber attacks, potentially up to and including the cyber attacks on Estonia, a pass at least as applied to international humanitarian law. This could encourage criminals, if all they have to worry about is law enforcement, and not the armed forces. Instead, and while the law of cyberwarfare remains malleable, the overall control standard should be adopted.

3.2 THE CASE FOR THE OVERALL CONTROL STANDARD

The ICJ has consistently used the more restrictive effective control standard in its jurisprudence, most recently in *Bosnian Genocide*, but other tribunals, such as the

ICTY, have not. Judge Antonio Cassese, the first President of The Hague Tribunal, attacked the B*osnian Genocide* judgment as demanding an "unrealistically high standard of proof" (Tosh, 2007). This burden of proof is nearly impossible to satisfy in the context of cyberspace without major improvements in the tracing of cyber attacks. As a result, if international law is to have sufficient applicability to cyberwarfare, it is essential that the overall control standard be adopted as part of a future international regime for cyberspace. Currently the framework for how such a treaty would operate is being debated, for the first time, by representatives of the United States and Russia. The two sides are far apart, but even preliminary discussions are encouraging (Markoff & Kramer, 2009). If these talks do bear fruit, their scope should be expanded to formulate a standard of State responsibility for cyber attacks.

Short of a new treaty on cyberspace, and alternatively to adopting the ICTY overall control standard, there is also precedent within the ICJ context itself to support a third more flexible standard of State responsibility. Specifically, the ICJ held in the *Iran hostage case* that the actions of a State's citizens could be attributed to the government if the citizens "acted on behalf on [sic] the State, having been charged by some competent organ of the Iranian State to carry out a specific operation" (United States v. Iran, 1980, p. 29). There, while the Court did not find enough evidence to attribute the actions of the citizens to the government, the Court did find that the Iranian government was nonetheless responsible because it was aware of its obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff, and failed to comply with its obligations (Barkham, 2001, p. 98).[3] This reasoning could be extended to cyber attacks in two ways. First, the standard could be adopted that, if the citizens of a State acted on behalf of a competent government organ, then the government could be vicariously liable for the resulting damage from such cyber attacks. Second, if there is insufficient evidence to find attribution outright, as there was in *Iran hostage*, then the standard could become one of governmental awareness, i.e. if the government was aware of its obligations under international law to prevent its citizens and information infrastructure from launching cyber attacks and failed to comply with these responsibilities. That State could then be held in breach of international law. Either the *Tadic* or *Iran hostage* standards has the benefit of moving beyond the rigid effective control framework, and holding State sponsors

3 The *Corfu Channel* case should also be considered in this context. In that case, Albania mined the Corfu Strait, and the British Royal Navy sued for damages and loss of life that it sustained as a result of ships colliding with the mines. There, the ICJ stated: "…it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein." (United Kingdom v. Albania, 1949, p. 30). Yet, even in *Corfu Channel* the Court noted that the standard of State responsibility should be somewhat flexible when it stated, "…the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence." (United Kingdom v. Albania, 1949, p. 30).

of cyber attacks accountable when significant evidence exists of their involvement.

Yet there are difficulties posed by adopting a standard of State responsibility with a lower burden of proof than effective control that should be addressed. Principal among these is the danger of prosecuting accused State sponsors of attacks that are in fact innocent. Politically, this worry may cause some countries to push for the higher burden of proof enshrined in the effective control standard so as not to be wrongly accused of sponsorship. Such critiques may in part be addressed though by a clarification that a requirement of 'beyond a reasonable doubt' under the overall controls standard is still a very high burden of proof that the prosecuting entity must meet, making frivolous or unwarranted cases unlikely (Erikkson, 2004, p. 294). Other outstanding issues that demand attention include the necessity of defining the appropriate forum in which to bring a case against State sponsors of cyber attacks, with candidates ranging from the ICJ, to national courts, or specialized tribunals.

In summary, it is far too easy for governments to hide their information warfare operations under the effective control standard. It should thus be sufficient as matter of international law to prove overall control by a government in a cyber attack, rather than complete control. For example, if the overall control standard were used instead of effective control, it would be possible that Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution. A comprehensive future legal regime could grant Estonia, and other victim nations, adequate reparations for such attacks. But if effective control becomes the dominant paradigm for determining State responsibility for cyber attacks, even a victim State of a worst-case scenario cyber attack may not receive justice. Alternatively, the ICJ precedent of *Iran hostage* could be used as another vehicle to hold State sponsors of cyber attacks accountable. But why is this distinction critical within the context of NATO's cyber security strategy?

4. CYBER CONFLICTS AND NATO

During the 2007 cyber attack on Estonia, several Estonian officials raised the issue of whether Article 5 of the North Atlantic Treaty Organization (NATO) could be invoked, which maintains that an assault on one allied country obligates the alliance to attack the aggressor (*North Atlantic Treaty,* 1949 art. 5). This was the first time in NATO history that a member State had formally requested emergency assistance in the defense of its digital assets (Hughes, 2009). Estonia did receive the limited help that it requested from NATO. Further assistance was unavailable since NATO and the international community alike viewed the 2007 cyber attacks on Estonia as an instance of cyber crime, or cyber terrorism (Koms & Kastenberg, 2008-09, p. 63).

This was also the case in the cyber attacks against Georgia, in which there was also no conclusive evidence that Russia was indeed behind the attacks (Schapp, 2009, p. 121). This was for two primary reasons. First, the attacks were not serious enough to constitute an armed attack thus activating NATO Article 5. Second, State responsibility for the attacks could not be conclusively proven. NATO has taken steps to address the gaps in cyber security strategy that the cyber attacks on Estonia underscored, such as by creating the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, and the new Cyber Defense Management Authority in Brussels, which is a NATO effort to centralize cyber defense capabilities ("NATO opens new centre of excellence on cyber defence," 2008). But without a legal regime for State responsibility in place going forwards, such efforts are by themselves insufficient.

It is critical for NATO's future efforts in cyber security for its member States to have a comprehensive and settled standard to gauge State responsibility for cyber attacks. Specialists at the CDMA, or at the various CERTs of the member States, will not be able to gather the necessary intelligence to prove which nation or group launched a given cyber attack if the standard of proof itself is left undefined. If the effective control standard is indeed accepted as the required standard for State responsibility, then information gathering would have to be total, necessitating new technologies capable of tracking individual packets conclusively back to their true source. Alternatively, if the overall control standard is adopted by the international community, then significant evidence beyond a reasonable doubt of State sponsorship or support for cyber attacks would be sufficient to hold accountable those States, or groups within those States, that launch cyber attacks against NATO member nations or businesses operating within member States.[4] Thus, it is in NATO's own best interests to have a standard of State responsibility for cyber attacks defined, and to push for the adoption of the overall control standard over the effective control standard.

5. CONCLUSION

The domestic and global implications of human society's increasingly critical dependence on the Internet makes necessary the ability to deter, detect, and minimize the effects of cyber attacks (Lipson, 2002, p. 3). Today, NATO and the United States alike are at the point of determining how the governance of cyberspace should develop, including influencing the vector of the *jus ad bellum* from the very inception of the legal framework for cyberwarfare. The strategies and practices that are assumed in the short-term thus will greatly impact how this fast evolving body of law is shaped (Schmitt, 2003, p. 415). The case has been made in this Article that there

4 A recent well-publicized example of such a case was the cyber attack on Google in which there were questions over Chinese-government sponsorship (Shiels, 2010).

are currently two vying regimes for State responsibility under international law: the effective and overall control standards. Due to the technical difficulties with proving attribution for cyber attacks, along with the unreasonably high standards of proof imposed by the effective control standard, I have argued for the adoption of the overall control standard. This has the benefit of holding State sponsors of cyber attacks accountable where there exists sufficient proof beyond a *reasonable* doubt, as opposed to beyond *any* doubt. Adopting the overall control standard for cyber attacks is thus both within the best interests of NATO and the international community. But determining a standard for State responsibility is only one part of promoting cyber security. There are a myriad of other related issues that deserve further research and attention by scholars and policymakers alike, such as determining the appropriate forum in which to prosecute State sponsors of cyber attacks.

REFERENCES

- Barkham, J., 2001. Information Warfare and International Law on the Use of Force. *New York University Journal of International Law and Policy,* 34, 57-114.
- Brenner, S. W., & Crescenzi, A. C. 2006. State-Sponsored Crime: The Futility of the Economic Espionage Act, *Houston Journal of International Law, 28, 389-464.*
- Burgess, D. R., 2006. Hostis Humani Generi: Piracy, Terrorism and a New International Law, *University of Miami International and Comparative Law Review, 13, 293-312.*
- Capaldo, G. Z. 2007. Providing a Right of Self-Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict, *Harvard International Law Journal Online, 48, 101-112.*
- Cassese, A. 2007. The *Nicaragua* and *Tadic* Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, *European Journal of International Law, 184, 649-668.*
- Cordesman, J. 2002. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection.* Westport: Praeger Publishers.
- Davis, J. 2007, August 21, Hackers Take Down the Most Wired Country in Europe. *Wired Magazine*, p. 9.
- Erikkson, S. 2004. Humiliating and Degrading Treatment under International Humanitarian Law: Criminal Accountability, State Responsibility, and Cultural Considerations, *Air Force Law Review, 55, 269-311.*
- Gray, C. 2000. *International Law and the Use of Force.* Oxford: Oxford University Press.
- Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271, T.S. 598 1907, *entered into force* 26 Jan. 1910, art. 1.
- Hanseman, R. G. 1997. The Realities and Legalities of Inform The Realities and Legalities of Information Warfare, *United States Air Force Law Review, 42, 173-200.*
- Held, D. 2006. *Models of Democracy.* Cambridge: Polity Press.
- Hughes, R. B. 2009, April, NATO and Cyber Defence: Mission Accomplished?. *NATO-OTAN.*
- Hunter, D. 2003, Cyberspace as Place and the Tragedy of the Digital Anticommons, *California Law Review, 91, 439-514.*
- "Internet: General Usage Statistics," http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/internet.htm.
- Janczewski, L. & Colarik, A. M. 2008. *Cyber Warfare and Cyber Terrorism*, Cambridge: CUP, 2008.
- Johnson, D. & Post, D., 1996, Law and Borders – The Rise of Law in Cyberspace, *Stanford Law Review, 48, 1367-1402.*
- Joyner, C. C. & Rothbaum, W. P., 1993, Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?, *Michigan Journal of International Law, 14, 220-260.*
- Koms, S. W. & Kastenberg, J. E., 2008, Georgia's Cyber Left Hook, *Parameteres—U.S. Army War College Quarterly, 38, 60-76.*
- Lessig, L. 1999, The Law of the Horse: What Cyberspace Might Teach, *Harvard Law Review, 113, 501-549.*
- Lipson, H. F. 2002, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, *CERT Coordination Center.*
- Luban, D. 2007, February 15, Timid Justice: The ICJ should have been harder on Serbia, *Slate.*
- Lulasik, S. 2003. *Protecting Critical Infrastructures Against Cyber-Attack.* Oxford: Oxford University Press.
- Markoff, J. & Kramer, A. E. 2009, December 12, In Shift, U.S. Talks to Russia on Internet Security, *New York Times.*

- Military and Paramilitary Activities Nicar. v. U.S. 1986 I.C.J. Rep. 14 Jun. 27.
- NATO 2008, May 20, NATO opens new centre of excellence on cyber defence, *NATO News.*
- North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241U.N.T.S. 243.
- Pronk, R. J.P. 1997, ICTY Issues Final Judgment Against Dusan Tadic in First International War Crimes Tribunal Since World War II, *Human Rights Brief, Center for Human Rights and Humanitarian Law.*
- Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 Oct. 2, 1995.
- Reich, R. B. 1991. *The Work of Nations: Preparing Ourselves for 21st-Century Capitalism.* New York: Vinage Press.
- Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 Dec. 12, 2001.
- Russian-Estonian MLAT.
- Ryan, J. 2007. *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web.* Dublin: IIEA.
- Schmitt, M. N. 2003, The Sixteenth Waldemar A. Solf Lecture in International Law, *Military Law Review, 176, 364-421.*
- Schmitt, M. N. 1998, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law, 7, 885-937.*
- Schapp, A. J. 2009, Cyberlaw Edition: Cyber Warfare Operations, Development and Use Under International Law, *Air Force Law Review, 64, 121-173.*
- Shackelford, S. J. 2010, Estonia Three Years Later: A Progress Report on Combating Cyber Attacks, *Journal of Internet Law, 138, 22-29.*
- Shackelford, S. J. 2009, From Net War to Nuclear War: Analogizing Cyber Attacks in International Law, *Berkeley Journal of International Law, 25, 191-250.*
- Shackelford, S. J. 2007, Holding States Accountable for the Ultimate Human Rights Abuse: A Review of the ICJ Bosnian Genocide Decision, *Human Rights Brief, 14, 21-26.*
- Shiels, M. 2010, 14 January, Security Experts say Google Cyber-Attack was Routine, *BBC News.*
- The Application of the Genocide Convention Case Bosnia and Herzegovina v. Serbia and Montenegro, 2007 I.C.J. 140 Feb. 26.
- The Corfu Channel Case United Kingdom-Albania, 1949 I.C.J. 4ff.
- Tosh, C. 2007, March 2, Genocide Acquittal Provokes Legal Debate, *Institute for War and Peace Reporting.*
- United States Diplomatic and Consular Staff in Tehran U.S. v. Iran, 1980 I.C.J. 3, 29 May 24.
- U.S. Department of State 2007, *Treaties in Force* http://www.state.gov/s/l/treaty/treaties/2007/index.htm
- Verton, D. 2003. *Black Ice: The Invisible Threat of Cyberterrorism.* Cambridge: CUP.
- Watkin, K. 2004, Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, *American Journal of International Law, 98, 1-34.*
- White House 2003. *National Strategy to Secure Cyberspace,* 19.
- Wolf, J. B. 2000, War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, *American Criminal Law Review, 28, 95-117.*
- Yang, D. W. 2006, Countering the Cyber-Crime Threat, *American Criminal Law Review, 43, 201-215.*