Intervention in national and private cyberspace and international law

Pål Wrange

Professor of International Law, Stockholm University
Director, the Stockholm Center for International Law and Justice
pal.wrange@juridicum.su.se

Published in Jonas Ebbesson, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds), International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi, (Leiden: Brill/Nijhoff, 2014) 307-326.

1 Introduction

The NSA affair has raised the issue of surveillance in cyberspace on the international agenda.[1] The first media reports in June 2013 concerned data collection by the US National Security Agency of domestic and international telephone calls as well as of Internet traffic, but subsequent reports have revealed that the NSA has also been involved in 'hacking" into government computers of foreign states. Even though this has sparked a bit of a debate between international lawyers as to the lawfulness of these activities,[2] until now, international legal doctrine has not had very much to say on these matters.

[1] To future readers: This refers to surveillance of American and global computer and telephone traffic by the US National Security Agency and other agencies, revealed through a series of leeks from former NSA contractor Edward Snowden, and usually published in The Guardian (and subsequently also elsewhere). See The Guardian's webpage on NSA, <http://www.theguardian.com/world/prism>, accessed 31 March, 2014.

[2] See the recent debates on EJIL Talk! and Opinio Juris: Anne Peters, 'Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Parts I & II,' http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/, accessed on 20 November, 2013; Peter Spiro, 'NSA Files: An Emerging Human Right to Privacy?', http://opiniojuris.org/2013/10/29/nsa-files-emerging-human-right-privacy/, accessed on 20 November, 2013.

This essay will here argue that an intrusion by a state in foreign national cyberspace[3] may be prohibited even if it does not amount to the use of force, both as a violation of sovereignty and as a violation of human rights. That conclusion is arrived from the point of view of a generalist[4] through the application of existing international law.

2 Cyberspace and international law

The definition of a state under international law is a territory and a population represented by an effective government. While all three aspects of the state are important – without a government there cannot be a state, and the reason for the state is the well-being of the population – it is arguably the territory that is the single most important delimiting criterion. The territory effectively determines the population, and the most important demarcation of the government's legitimate power (its jurisdiction) is the territory. This territorial basis for political governance has been put in question by increased travel, migration and economic exchange, and governments now exercise at least some aspects of jurisdiction over considerable numbers of events abroad.

However, this complication is minor compared to those caused by the Internet. Even though governments are increasingly taking control over their national cyberspaces, and even though the principle of territoriality provides that a state has jurisdiction over servers and nodes within its recognized borders,[5] communication between servers and computers is routed in international webs mostly operated by private networks, which are not controlled by any one government,[6] and many virtual national assets are stored in servers abroad.

---

[3] For reasons that will be presented below, I use the unusual expression 'national cyberspace". I am aware that it might appear to be a contradiction in terms, and I further do not consider airspace to be perfect analogy. However, states do have sovereignty over hardware located within their territories. To what extent jurisdiction may and should be exercised is a more complex question, which will only partly be addressed here.

[4] Although I have concerned myself with cyber issues a few times since 2000, I do not consider myself to be a specialist. I am an international lawyer, and I apply the law to cyberspace just as I would to any other space.

[5] J Trachtman, 'Global cyberterrorism, jurisdiction, and international organization', (2006) *Grady, M.'The Law Econ. Cybersecurity* 10, ftp://24.139.223.85/Public/Tesis_2011/legal_etchics/Perceptions2/others/globalcyberterrorim.pdf (last accessed Nov 12, 2013). But cf JE Kastenberg, 'Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law' (2009) 64 *AFL Rev.* 43, 64, http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/airfor64&section=5 (last accessed 28 November2012).

[6] They are, however, partly under the control of the US Government. The domain names – like gov.se or gov.az – are controlled by thirteen clusters of domain name servers, ten of which are controlled by various

Business offers, opinions and fraudulent messages sent from one country and stored in a server in another country may effect events in a third country. Perhaps most importantly, national assets in cyberspace – public and private – can more or less easily be surveyed, affected or even controlled through cyber operations from foreign states, and in particular from a few very technologically advanced ones. This has led some observers to suggest that the Internet is beyond the sovereignty of governments,[7] or even a new dimension, not subject to the same regulation as other spheres of human activities.[8]

Nevertheless, the Internet and other computer networks have physical locations, under the jurisdiction of one or more states, and the actors have nationality, regardless of whether they are individuals or corporations.[9] In addition, cyberspace has been securitized, and states seek to protect their critical cyber infrastructure from criminal actors and political enemies. It is therefore only logical that states have asserted jurisdiction over computer networks, in an increasingly assertive way.[10] As a further corollary, international law as it currently exists, applies to computer networks.[11] This, too, is a position generally taken by states,[12] as confirmed in a report from a broadly representative group of

---

institutions in the United States, including three US government agencies. And the program for the top domains -- .se, ae, etc -- is controlled by a US corporation (VeriSign) under an agreement with the US Department of Commerce.

[7] One of the famous expressions of this view is John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996), http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration (last accessed 13 October 2013).

[8] Michael M. Schmitt, 'Cybserspace and International Law: The Penmbar Mist of Uncertainty', *Harvard Law Review Forum*, March 2013, http://www.harvardlawreview.org/issues/126/march13/forum_1000.php (last accessed Nov 12, 2013). For a very interesting analysis of issues related to jurisdiction, see T Schultz T, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 *European Journal of International Law* 799.

[9] Cf Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law' (2009) 88 *Tex. L. Rev.* 1571, 1573.

[10] On the possibilities of 'renationalization' of the Internet, see C Engel, 'The Role of Law in the Governance of the Internet' (2006) *Int. Rev. Law Comput. Technol.*1-16, 8; and E Tikk, *Comprehensive legal approach to cyber security* (2011) 102, http://dspace.utlib.ee/dspace/handle/10062/17914 (last accessed 13 October2013). See also Bernard Oxman, Jurisdiction of States, Encyclopedia of Public International Law, on-line version, accessed 31 March, 2014, para 31.

[11] See WH von Heinegg, 'Legal implications of territorial sovereignty in cyberspace', in *4th International Conference on Cyber Conflict* (C Czosseck, R Ottis, & K Ziolkowski eds., 2012) 7–19,9-10.

[12] The US Cyberstrategy provides:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace Nonetheless, unique attributes of networked technology require

governmental experts, which concluded i.a. the following in a UN report in June 2013:[13]

> '19. International law, and in particular the Charter of the United Nations, is applicable …
>
> 20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.
>
> 21. State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.
>
> ….
>
> 23. States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."

Still, the situation is far from clear. With the exception of the Budapest Convention against Cybercrime, and possibly some provisions in the ITU Convention[14] (drafted long before Internet), there is no international convention on the topic.[15] The aforementioned UN report – written by a group of experts -- is the closest thing we have to an authoritative intergovernmental opinion. There are very few instances of *opinio juris,* very little, if any, confirmed state practice, and no judgments or reports from international adjudicative or monitoring bodies. As mentioned, there is not even very much doctrine; most writers who

---

> additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.

United States. White House Office & B Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011) 9. http://scholar.google.se/scholar?q=%22INTERNATIONAL+STRATEGY++FOR+CYBERSPACE%22&btnG=&hl=sv&as_sdt=0%2C5#1 (last accessed Nov 9, 2013).

[13] UN General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,' A/68/98, June 24, 2013.

[14] See Chapter VI of the Constitution of the International Telecommunication Union as amended 2010, http://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx, accessed 31 March, 2014.

[15] In 2011, Russia proposed a 'Draft Convention on International Information Security', which has not met with general approcal. See comments by Conflict Studies Research Centre at http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf, accessed 31 March, 2014.

have engaged in international law aspects of cyber sphere have written about international humanitarian law and the use of force. One important exception is the Tallinn Manual, drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence and published in 2013, which deals expertly but briefly and not conclusively with some peacetime uses of Internet.[16]

3 Sovereignty and intervention in cyberspace

As implied above, the starting point must be that states exercise sovereignty over their respective cyberspaces,[17] *mutatis mutandis*. However, states may have many reasons to take measures also in foreign cyberspace. Some of these reasons are legitimate as such,[18] like investigations of and responses to terrorism and other crimes. Others may be more dubious, like intelligence or sabotage.

Many such measures are covered by various international conventions against transnational crime and terrorism. While these conventions do not allow intrusions, like unauthorized data access, in the jurisdictions of other states, they do mandate states to cooperate with one another, as does the Council of Europe's Convention on Cybercrime.[19] Counter-crime and -terrorism measures that take effect on foreign territory will therefore ideally be carried out in cooperation with local law enforcement officers under a convention or through an ad hoc agreement. However, such cooperation cannot always be secured. Therefore, a state may feel tempted to carry out law enforcement or counter-terrorism without proper authorization from the other state concerned.

This could involve search of information on private computers in order to prevent or investigate crimes and terrorism; an interdiction of a cyber-attack or a 'hack-back" in real time; or an attack aimed at deterring counter-strikes. A state could also manipulate bank accounts, plant false information, interrupt the functioning of critical information infrastructure or create a break-down in the financial system. Some of these measures may damage hardware and software, but even more of them will constitute unauthorized intrusions in computers and

[16] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (OUP 2013). For a critical discussion, see LJM Boer, ''Restating the Law 'As It Is'': On the Tallinn Manual and the Use of Force in Cyberspace' (2013) *Amsterdam Law Forum*; Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' (2013) 18 *Journal of Conflict and Security Law* 331.

[17] See footnote 3.

[18] Legitimate reasons do not, however, necessarily justify all means, as will be argued.

[19] See footnote 34.

servers or interfere with computer traffic, and may be in violation of international law, even if the purpose is legitimate.

Such acts may constitute armed attacks, illegal intervention, or legal countermeasures, while other acts are legally unproblematic. I will here discuss first, and only briefly, the use of force, then other forms of intervention, including countermeasures and self-help, thereafter present a few arguments on cyber espionage and lastly I will bring in human rights.

First of all, some acts in foreign cyberspace might amount to the use of force under Article 2(4) of the UN Charter, as is now a growing consensus among international lawyers.[20] There have been no known, clear examples of cyber intrusions that might amount to the use of force. The Stuxnet virus, launched in 2010 against Iran -- allegedly by US and/or Israel – is the most interesting example, so far. According to reports, it caused malfunction in or destroyed around 1000 centrifuges in the Iranian nuclear program.[21] If this could be attributed to a government, it would appear to constitute an act of force.[22]

As to the threshold, writers generally hold that cyber attacks (or computer network attacks) that cause considerable 'kinetic" damage constitute illegal use of force, or even an armed attack. There is, however, controversy regarding whether destruction of for instance software, including data, might constitute an armed attack; some writers think so, especially if great financial loss is incurred,[23] but others think differently:

> Computer-based espionage, intelligence collection, or even some preemptive cyber-operations or / countermeasures designed to disable an adversary's threatening capabilities, for example, would generally not constitute prohibited force because these activities do

[20] See Tallinn Manual (fn 16) 46 et seq.

[21] See, i.a., David P. Fidler, 'Revelations Concerning Cybersecurity, Recent Developments and Revelations Concerning Cybersecurity and Cyberspace : Implications for International Law', (2012) *ASIL Insight* 16; David P. Fidler, 'Was Stuxnet and Act of War? Decoding a Cyberattack' (2011) 9 *IEEE Security & Privacy Magazine* 56-59.

[22] Fleck D, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' (2013) 18 *Journal of Conflict and Security Law* 331, 332; R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 211, 221.

[23] See, for instance, Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing, The Hague 2012) 131 *et seq*; Schmitt M, 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 *Vill. L. Rev.* 569, 590; SJ Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkeley J. Int. Law* 192, 238.

> not produce destructive consequences analogous to a kinetic military attack.[24]

For many commentators, the discussion stops here. If an act does not constitute use of force, it appears to be more or less unproblematic. However, many of these acts, like espionage, may constitute illegal intervention or interference, and that issue has been subject to much less academic debate. As Mary Ellen O'Connel reminds us in a text on cyber security and international law,

> [i]nterference with a state's economic sphere, air space, maritime space, or territorial space, even if not prohibited by Article 2(4) of the UN Charter is prohibited under the general principle of non-intervention.[25]

Those writers who have commented specifically on the principle of non-intervention generally agree that the principle applies in cyberspace.[26] However, there is less commentary on the question to what extent acts in cyberspace that do not purport to coerce a state, but just infringe on sovereignty, are prohibited. As is well known, enforcement of a state's laws may not take place on another state's territory without that state's consent, and a state shall not exercise public authority on another state's territory. This was confirmed in very clear terms in a judgment from Canada's Supreme Court:

> The power to invade the private sphere of persons and property, and seize personal items and information, is paradigmatic of state sovereignty. These actions can be authorized only by the territorial state.[27]

As Jamnajed and Wood explain,

> Examples of prohibited extraterritorial enforcement jurisdiction include the collecting of evidence and police and other investigations (even if not purporting to use powers of compulsion) conducted without the consent of the territorial state.[28]

---

[24] Matthew Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)' (2011) *Yale Journal of International Law* 421, 434-435-

[25] Mary Ellen O'Connell, 'Cyber Mania', in *International Law: Meeting Summary: Cyber Security and International Law* (Mary Ellen O'Connell, Louise Arimatsu, & Elizabeth Wilmshurst eds., 2012) 3, 6.

[26] Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) *Journal of Conflict and Security Law* 223.

[27] R. v. Hape, 2007 SCC 26 (CanLII), (2007) 2 SCR 292, para 87. <http://canlii.ca/t/1rq5n> retrieved on 2013-10-18.

[28] Maziar Jamnejad & Michael Wood, 'The Principle of Non-intervention' (2009) 22 *Leiden J. Int. Law* 345, 372.

One simple rule of thumb is that acts that are prohibited for a private person (i.e. without public authority) are not allowed for a foreign state.[29] For instance, search of a home is illegal for a private person, and is thus prohibited.[30]

How does this apply in cyberspace? Even though most of the debate on governmental cyber attacks have concerned various forms of cyber warfare, it appears to be generally agreed that the principle of non-intervention, too, applies in cyberspace, as mentioned above. This means that international law limits the way states intrude into cyberspace of other states, even below the threshold of use of force. As Wolff Heinschel von Heinegg has noted, the U.S. International Strategy for Cyberspace finds that 'attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy' may qualify as violations of U.S. territorial sovereignty.[31]

This is confirmed by other writers.[32] However, there is controversy as to if intrusions that do not create any lasting harm are included. This is an issue that is relevant for the legal assessment of many measures undertaken in crime enforcement and intelligence collection. According to some writers, damage is irrelevant, whereas others find that only intrusions that cause material harm constitute illegal interventions.[33]

The latter view is difficult to understand, though. If a police officer from country A conducts an unauthorized search in a house or in postal communications in country B, then that a measure is illegal, even if no physical harm has occurred. That must surely apply also to servers or computers, and I have certainly seen no evidence of international customary or treaty law that would indicate an exception for searches on ICT machinery/gear. Under the Council of Europe's Budapest Convention on Cybercrime – which has been ratified also by some non-

---

[29] Michael Akehurst, 'Jurisdiction in International Law' (1972) 46 *Brit. YB Int'l L.* 146.

[30] Perhaps the principle of non-intervention goes even further and excludes all forms of investigations by law enforcement authorities on foreign soil.

[31] WH von Heinegg, 'Legal implications of territorial sovereignty in cyberspace', in *4th International Conference on Cyber Conflict* (C Czosseck, R Ottis, & K Ziolkowski eds., 2012) 7–19, 11 & 12, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last accessed 13 October2013).

[32] C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) J. Nat'l Sec. L. Pol'y 179, 201. See also T Tuukkanen, *Sovereignty in the Cyber Domain*, *in The Fog of Cyber Defence* (Jari Rantapelkonen & Mirva Salminen eds., 2013) 37 http://www.academia.edu/download/30888836/The_Fog_of_Cyber_Defence_NDU_2013.pdf#page=38 (last accessed 13 October2013).

[33] WH von Heinegg, 'Legal implications of territorial sovereignty in cyberspace', in *4th International Conference on Cyber Conflict* (C Czosseck, R Ottis, & K Ziolkowski eds., 2012) 7–19, 11, 12 & 16, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last accessed 13 October2013).

European countries, including the US – a number of acts, commonly conducted as a part of law enforcement or cyber espionage (see below), are criminalized. This includes illegal access and illegal interception, and the Convention contains no exceptions for measures taken by foreign public agencies. In fact, the preparatory works of the Convention clearly spell out that the Convention does not allow remote extraterritorial search.[34] This also seems to be the position taken by for instance US domestic law enforcement agencies.[35] Hence, the logical conclusion is that the general prohibition of intervention, including the prohibition of infringements on territorial sovereignty, applies also in cyberspace.

It is sometimes argued that operations that take place from locations outside the target country are not illegal.[36] Therefore, the argument goes, it is the laws of the state from which the remote search takes place that should determine whether the act is legal. This conclusion, however, flies in the face of the basic principles of jurisdiction. States usually include under their jurisdiction not only acts which are *commenced* within their territories but also acts that *take effect* within that territory.[37] In addition, many states assume jurisdiction also over crimes that affect the national security of a state. Hacking into servers and other computers of state A affects state A in a tangible way.[38] Therefore, states my assume jurisdiction over such crimes, and indeed have done so. Hence, the argument that the law enforcement officer (or the spy) is physically located abroad does not seem to hold. S/he is still committing a crime in the target state and hence an illegal infringement of sovereignty.

---

[34] AM Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 *Berkeley Tech. LJ* 425, 433. See also convention Art 32 of the Budapest Convention; Convention on Cybercrime, Council of Europe, ETS No 185, available at www.coe.org. Another argument against such intrusions, provided by Shackelford, is that '(t)he ITU Constitution militates against 'harmful interference,' defined in the Annex 3 of the document as that which 'endangers . . .safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations.' SJ Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkeley J. Int. Law* 192, 223.

[35] See also SW Brenner & JJ Schwerha IV, 'Transnational evidence gathering and local prosecution of international cybercrime', (2001) XX *J. Marshall J. Comput. Info. L.* 347–395, 386-388. However, for differences between the more 'liberal' US approach and that of other states, see Ray August, 'International Cyber-Jurisdiction: A Comparative Analysis' (2002) 39 *Am. Bus. Law J.* 531–573, 561-564. For an example of extraterritorial seizure in Russian computers (in violation of international law), see Kenneth Geers, 'Extra Territoriality and International Cyber Crime' *(2005)* 3 *The CIP report No 7* 7-11.

[36] J Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (2001) *Univ. Chicago Leg. Forum*, http://essays.ssrn.com/sol3/essays.cfm?abstract_id=285732 (last accessed 28 November2012).

[37] See Ray August, 'International Cyber-Jurisdiction: A Comparative Analysis' (2002) 39 *Am. Bus. Law J.* 531–573, 537.

[38] See also August *ibid* 535.

Nevertheless, even if unauthorized, under some circumstances such measures may be justified as countermeasures and/or as self-help. First of all, a state may take countermeasures against attacks from another state, and that applies even if the attack does not reach the threshold of an armed attack or even use of force. Article 22 of the International Law Commission's Draft Articles on State Responsibility provides that '[t]he wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State.' This applies on certain conditions, for instance that the purpose must be to 'induce that State to comply with its obligations.[39] Hence, the purpose may not include 'punishment' or the preventive destruction of the means through which the attack has occurred. So, for instance, if the Stuxnet virus could be attributed to a particular state, then Iran could take countermeasures against that state, but only in order to stop the attack or, possibly, to stop further attacks.[40]

In addition to countermeasures, which may only have the aim of inducing the target state to comply with its obligations, states may also invoke necessity, if that '[i]s the only way for the State to safeguard an essential interest against a grave and imminent peril'.[41] However, there is no general mandate to take self-help measures.

Several of the most famous incidents, like the attacks against Estonia in 2007[42] and against Georgia in 2008,[43] have been difficult to impute directly to a state. It is generally very difficult to attribute a cyberattack to a particular subject in real

---

[39] Article 49, Draft Articles on State Responsibility.

[40] Unless another rule of international law would legalize Stuxnet, which I doubt

[41] Article 25 of the ILC Draft Articles provides:

> 1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:
>
> (*a*) Is the only way for the State to safeguard an essential interest against a grave and imminent peril; and
>
> (*b*) Does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

[42] Schmitt believes that it reached threshold of use of force, whereas Buchanan finds otherwise, but holds that the attacks nevertheless reached the threshold of illegal coercion. 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 *Vill. L. Rev.* 569, 578; Buchanen See R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 211, 218-219.

[43] E Tikk, *Comprehensive legal approach to cyber security* (2011) 42-43, http://dspace.utlib.ee/dspace/handle/10062/17914 (last accessed 13 October2013).

time. This, of course, makes it difficult to determine what reactions are appropriate and legal.[44]

In principle, a state may be responsible for acts carried out by individuals, if these individuals are directed or controlled by a state or if the state in question adopts those acts as its own.[45] This means that a state that harbors and actively assists terrorists or other criminals may be legally responsible for their acts.[46] If terrorists are involved in acts on a large scale and if the assistance is substantial – beyond financing – such a government may be responsible for use of force or even for an armed attack.[47] Furthermore, a state has the duty 'not to allow knowingly its territory to be used for acts contrary to the rights of other States."[48] That obligation includes the duty to investigate and prosecute, in cooperation with the target state, as well as a measure of active prevention.[49] A state is not responsible, however, if it could not know and if it could not prevent.

---

[44] Eneken Tikk is less pessimistic. '(A)ttribution as an issue is not to be generalised, since different standards for attribution and relevant legal consequences exist – – to restrict access to communications in case of a malicious activity there is no need to identify the actor – it is sufficient to point out the device; – to request cooperation from or to impose economic sanctions against a country that lets its cyber infrastructure be used for routing cyber attacks there is no need to attribute the attacks to any specific person – it suffices to define which networks/operators are involved and which jurisdiction they belong to; – to engage in collective self-defence against a nation state, the decisive factor is the level of hostilities.' E Tikk, *Comprehensive legal approach to cyber security* (2011) 105, http://dspace.utlib.ee/dspace/handle/10062/17914 (last accessed 13 October2013). In my view, this is to simplify the problem somewhat. For instance, in order to engage in self-defense, even against a non-state actor, it is necessary to determine the level of state responsibility of the acts, and also to properly identify the 'real' sources of the attacks.

[45] See The International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Annex to United Nations General Assembly, Resolution 56/83 (2001). Article 8 reads:

> The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct.'

Article 11 provides that

> (c)onduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

Schmitt finds that the threshold for responsibility is lower. Michael Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 *Vill. L. Rev.* 569, 599.

[46] See Rule 11, the Tallinn Manual (fn 16). Cf also note 51.

[47] The Definition of Aggression, General Assembly Resolution 3314 (1974), Annex, Paragraph 3 (g).

[48] Corfu Channel Case, Judgment of April 19th, 1949, ICJ Reports 4 at 22 (1949).

[49] WH von Heinegg, 'Legal implications of territorial sovereignty in cyberspace', in C Czosseck, R Ottis, & K Ziolkowski (eds) *4th International Conference on Cyber Conflict* (2012) 7–19, 16, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last accessed 13 October2013)..

It is unclear to what extent a state is supposed to survey its cyberspace.[50] It is submitted, though, that if a state whose territory is being used for attacks is being notified and still does not take action in good faith, there is at least some degree of responsibility. A related question is if this obligation applies only to the hardware from which the attack is launched, or also to any lines through which the attack may be routed.[51] The response must be that the responsibility is the same, but the expected level of care must be gauged to take account of the technical difficulties involved. These important issues are unsettled, and as mentioned they relate to the possibility to resort to countermeasures.

At any rate, if a state is unable to police its portion of cyberspace, that might invite other states to take self-help measures. One commentator finds that '[n]o strict prohibition precludes preemptive government use of cyber-force as long as the perceived threat is demonstrated to be real and immediate, and the state adheres to the criteria of proportionality and necessity in applying computer-generated coercion.'[52] This finding is controversial, but there is at least some room for the invocation of necessity, as has been mentioned above.

---

[50] The comment to the Tallinn Manual reads: '11. The International Group of Experts could not achieve consensus as to whether this Rule also applies if the respective State has only constructive ('should have known') knowledge. In other words, it is unclear whether a State violates this Rule if it fails to use due care in policing cyber activities on its territory and is therefore unaware of the acts in question. Even if constructive knowledge suffices, the threshold of due care is uncertain in the cyber context because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets, and the ease with which deception can be mounted through cyber infrastructure.' The Tallinn Manual (fn 16). See also Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law' (2009) 88 *Tex. L. Rev*. 1571, 1591.

[51] The comment to the Tallinn Manual reads: '12. Nor could the International Group of Experts achieve consensus as to whether this Rule applies to States through which cyber operations are routed. Some Experts took the position that to the extent that a State of transit knows of an offending operation and has the ability to put an end to it, the State must do so. These Experts took notice, however, of the unique routing processes of cyber transmissions. For instance, should a transmission be blocked at one node of a network, it will usually be rerouted along a different transmission path, often through a different State. In such a case, these Experts agreed that the State of transit has no obligation to act because doing so would have no meaningful effect on the outcome of the operation. Other Experts took the position that the Rule applied only to the territory of the State from which the operation is launched or to territory under its exclusive control. They either argued that the legal principle did not extend to other territory *in abstracto* or justified their view on the basis of the unique difficulties of applying the Rule in the cyber context.' The Tallinn Manual (fn 16). So, both groups actually ended up with the same conclusion, that there is no responsibility. I am not convinced that either of them is correct, but it would lead to far to take up that argument in this context.

[52] SJ Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkeley J. Int. Law* 192, 237-238, http://works.bepress.com/scott_shackelford/5/ (last accessed 28 November2012).

4 Espionage

One particularly controversial – and surely prevalent -- type of Internet activity is cyber espionage. Espionage, or secret intelligence, is to obtain information 'covertly—that is, without the consent of the State that controls the information.'[53] To collect information is – in and of itself – not illegal under international law. According to one dictionary, espionage 'can involve the analysis of diplomatic reports, publications, statistics, and broadcasts, as well as spying, a clandestine activity carried out by an individual or individuals working under secret identity to gather classified information on behalf of another entity or nation.'[54] Many of these activities, which are now to a large extent carried out over the Internet, are legal, and do not need the consent of the target government.

However, espionage may also involve unauthorized intrusion into servers that contain private and secret data. In May in 2012, it was recorded that the spyware Flame had infected 1000 computers, with the majority of targets in Iran. Flame can 'record audio, screenshots, keyboard activity and network traffic... This data, along with locally stored documents, is sent on to one of several command and control servers that are scattered around the world.'[55]

Doctrine used to be divided between the view that espionage is not regulated by international law and the view that it is illegal, the latter view most forcefully argued by Quincy Wright.[56] In particular lately, some writers – notably quite a few American commentators – have argued that espionage is legal under international law (in spite of being prohibited by domestic law),[57] and that there

---

[53] Simon Chesterman, Secret Intelligence, *Encyclopedia of Public International Law*, on-line version, accessed 7 December, 2012.

[54] www.freedictionary.com.

[55] David Lee, 'Flame: Massive Cyberattack Discovered, Researchers Say' (28 May 2012) BBC News.

[56] Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in *Essays on Espionage and International Law* (Roland Stanger ed., 1962) 11. See C Forcese, 'Spies Without Borders: International Law and Intelligence Collection', *J. Nat'l Sec. L. Pol'y* (2011) 179, 202. See also S Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) *Michigan J. Int. Law* 1071, 1074-75.

[57] Lin H, 'Offensive Cyber Operations and the Use of Force' *J. Nat'l Sec. L. & Pol'y* (2010) 63, 72, 78; WH von Heinegg, 'Legal implications of territorial sovereignty in cyberspace', in *4th International Conference on Cyber Conflict* (C Czosseck, R Ottis, & K Ziolkowski eds., 2012) 7–19, 11, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962, accessed 13 Octover, 2013).

See also Alexander Melnitzky, 'Defending America against Chinese Cyber Espionage through the Use of Active Defenses' (2012) 20 *Cardozo J. Int'l Comp. L.* 537, 564.

is therefore no obstacle to committing espionage over the Internet.[58] Those who make that argument essentially say that espionage is not prohibited and/or that there is a universal custom to engage in espionage.[59] I will deal with each of those two arguments.

First, these writers point out that there is no treaty prohibiting espionage. Hence, if it is not prohibited, it must be legal. However, this argument misses the point that even though there is no wholesale prohibition of espionage, many more concrete forms of espionage are prohibited. Under Article 41(1) the Vienna Convention on Diplomatic Relations, for instance, states have undertaken the obligation that staff of diplomatic missions – many of which are in reality spies – must comply with domestic law in the state where they are being stationed. Other state agents are covered by the general prohibition of intervention, including the prohibition of enforcement. Some would argue that the prohibition of law enforcement abroad does not cover espionage. However, I can see no reason for why measures undertaken for security and intelligence purposes should be treated differently from measures undertaken to punish and prevent crime, and I am not aware of any legal sources that indicate that.[60]

The second argument provided by those who hold that *all* espionage is legal is that there is a customary norm to that effect, since all nations engage in such activity.[61] However, there are several counterarguments, and the most important

---

See also the review in C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) *J. Nat'l Sec. L. Pol'y* 179, 204.

[58] AJ Schaap, 'Cyber Warfare Operations: Development and Use Under International Law' (2009) 64 *AFL Rev.*, 121, 140-141, http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/airfor64&section=8, visited 28 November, 2012).

[59] 'No treaties or other sources of international law specifically prohibit espionage. International law does require respect for the territorial integrity of other states, but states have practiced territorially intrusive intelligence collection by air, sea, and on land, through a variety of means, from time immemorial. The domestic law of almost every state promotes the territorially intrusive collection of foreign intelligence by its own agents. As long as unexpressed but generally accepted norms and expectations associated with espionage are observed, international law tolerates the collection of intelligence in the territory of other nations.' Roger Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 *The Air Force Law Review* 219, 226.

[60] Another potential distinction that could be made in order to justify espionage is that between intrusion in private and public property, respectively. Again, I am not aware of any legal sources indicating the relevance of that distinction. By the way, it is likely that most governments would find it even more important to guard public property, at least in the context of non-intervention. The protection of diplomatic premises, archives and correspondence in the Vienna Convention on Diplomatic Relations certainly suggest that.

[61] This is implied by von Heinegg: Since all States engage in espionage, including via the cyberspace, mere intrusions into foreign computers or networks are not covered by the prohibition.' (2012) 7–19, 16, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962, accessed 13 October2013.

one is that this is based on a complete misunderstanding of how customary international law is formed. (Remember that the default position is that a number of types of acts conducted in the course of espionage are illegal, so the burden of proof is on those who claim that there is an exception for espionage.) In order for a customary norm to be formed, there needs to be not only state practice, but also *opinio juris*, a legal conviction that this practice corresponds to the law. I know of no state that has publicly claimed that espionage in all its forms is legal.[62] On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof.[63]

Both of the arguments for espionage assume that there is a special legal category of espionage. That is not the case, however. Therefore, like for so many other categories of human activities, the various acts of espionage have to be subsumed under established heads of legal terminology, to be assessed, each on its own merits. This does not mean that state practice is completely without legal consequences. The old saying *tu quoque* ('you, too') is relevant,[64] in that espionage by one state may be considered to be an estoppel against that state if it raises a claim against another state that engages in similar conduct.[65] However, that does not apply to third parties, including third states and individuals, who have not been engaged in espionage against that state.

I therefore conclude that espionage that involves unauthorized access to servers and other computers in a foreign state generally constitute illegal interventions into the sovereignty of that state.[66] This, of course, applies even more to covert

---

[62] The US Government made some statements to that effect in conjunction with the U2 incident in 1960, but that was, of course, after the plane had been shoot down.

[63] 'Even if it is commonplace, spying is a poor candidate for a customary international law exception to sovereignty – whatever state practice exists in the area is hardly accompanied by opinio juris.' C Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) *J. Nat'l Sec. L. Pol'y*. Tuukkanen is undecided. T Tuukkanen, 'Sovereignty in the Cyber Domain', in *The Fog of Cyber Defence* (Jari Rantapelkonen & Mirva Salminen eds., 2013) 37, 43 http://www.academia.edu/download/30888836/The_Fog_of_Cyber_Defence_NDU_2013.pdf#page=38 (last accessed 13 October2013).

[64] I am grateful to Professor Sundberg for having raised this argument. On the relevance of this argument in relation to the U2 incident, see Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in *Essays on Espionage and International Law* (Roland Stanger ed., 1962) 19.

[65] Cf Cherif Bassiouni, *Crimes Against Humanity in International Criminal Law* (2nd edn, Kluwer Law, 1999) 502.

[66] I had originally formulated this as 'crimes against the domestic law' with the caveat for (undefined) situations where the relevant domestic law of the target state is in violation of human rights. This view is supported by Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in *Essays on Espionage and International Law* (Roland Stanger ed., 1962) 12. As pointed out by Martin Ratkovich, that formulation may give too much leeway for states to unilaterally determine the threshold for illegal intervention.

operations or preparations for war which involve destruction of or tampering with data.[67]

5 Human rights

So, unauthorized access into computers in foreign states is generally illegal under international law, but may sometimes be justified. However, it is important to note that human rights cannot be disposed of by the state of nationality of the person in question. Hence, if state A conducts a search on the computer of an individual in state B, it is immaterial whether A invokes the consent of B or whether the measure is justified as a countermeasure. This is made clear by Article 50 of the International Law Commission's Draft Articles on State Responsibility: 'Countermeasures shall not affect: … Obligations for the protection of fundamental human rights.'

One highly relevant human right is the freedom of information, which is included under the freedom of expression, covered by Article 19 in both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). While a state has the right to close its borders – including borders in cyberspace – it must still respect the right to 'receive and impart information and ideas of all kinds, regardless of frontiers'. This means that any efforts that a state may take in order to counter terrorism or other crimes, for instance by stopping the dissemination of private or public messages from a computer, will have to take this right into account.[68]

This essay will be more concerned with another aspect, namely the right to privacy, protected under Article 12 of the UDHR and Article 17 of the ICCPR. Article 17 of the ICCPR provides:

---

[67] It is a different matter, however, if signals have been intercepted on the territory of the intercepting state or on the high seas or in outer space. However, in such cases international telecommunications law may be relevant, as noted by Forcese: 'It is difficult to see how the interception of electronic leakage from one state from the territory of another state violates a sovereignty interest. It is true that in respect to this sort of intelligence collection at least one additional legal instrument relating to transnational telecommunications may be relevant: the International Telecommunications Convention provides that members will 'take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.' C Forcese, 'Spies Without Borders: International Law and Intelligence Collection', 5 *J. Nat'l Sec. L. Pol'y* (2011) 179, 208

[68] The same applies to messages intercepted in the territory of the intercepting state or on the high seas or in outer space (or in Antarctica).

On Internet and the freedom of expression, see Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34, in particular paragraphs 43 & 44.

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

This applies in cyberspace, too. An intrusion by a state into a server in another state may constitute not only a violation of that other state's sovereignty, but also a violation of the human rights of another person. Article 17 does not prohibit all interference – interference shall not be arbitrary or unlawful, which suggests that a balance needs to be struck. The Human Rights Committee has explained this in the following words:

> 7. As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. …
>
> 8. Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis. Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited. …

This may be a little bit too strict for some states' tastes, and the general recommendations are not legally binding. They are, however, interpretations of the Covenant made by the competent international organ, and a state that wants to act differently should make a convincing counterargument.[69] The Committee

[69] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).

has recently, in the context of NSA surveillance, confirmed that Article 17 applies also to cyberspace.[70]

It may be argued that the ICCPR does not protect individuals who are situated beyond the territory of a state which invades their private spheres.[71] Article 2(1) of the ICCPR reads:

> 1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind...

Some commentators and states have argued that this means that the Covenant applies only to persons that are both in the territory of a state and under its jurisdiction, thus excluding, all persons abroad (as well as persons in the territory but subject to the jurisdiction of someone else, for instance an occupying power). This is, however, a misreading of the provision. Grammatically, the provision is divided into two obligations:

a) Each State Party to the present Covenant undertakes to respect …. the rights recognized in the present Covenant, without distinction of any kind…
b) Each State Party to the present Covenant undertakes … to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind…

This is completely logical. To *respect* mean essentially to not actively deny someone a right, which is something that a state has the power to do wherever it acts. The wider duty to *ensure* the right, on the other hand, can only be effectively complied with where the state is in charge.[72] The Human Rights Committee has

---

[70] Human Rights Committee, Concluding observations on the fourth report of the United States of America, advance unedited version, 2014, CCPR/C/USA/CO/4, para 22.

[71] See for example the view of Miquelon-Weismann, who is concerned with individuals in Europe who are being searched from the US, and finds that the US Bill of Rights does not apply to Europeans situated in Europe and that the European Convention on Human Rights does not bind the US, but who apparently is not aware that the US is bound by the ICCPR, which applies in both Europe and the US. The US is not likely to hold that human rights obligations apply outside US territory. Miriam F. Miquelon-Weismann, 'The Convention on Cybercrime: a Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?', 23 *J. Marshall J. Comput. Info. L.* (2004) 329, 357-358.

[72] It has recently been revealed that the then legal advisor in the US State Department, Harold Koh, had a similar view, and tried to change the more restricted US reading of the Covenant. 'Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights', US State Department, October 19, 2010, accessed at https://www.documentcloud.org/documents/1053853-state-department-iccpr-memo.html, accessed 31 March, 2014. See in particular page 4. See also the debate in March 2014 on www.ejiltalk.org and www.lawfareblog.com.

confirmed this dichotomy and has further confirmed that the convention has extraterritorial application, though not in exactly the same terms.[73] In the case López Burgos v Uruguay, the Human Rights Committee held that

> Article 2 (1) of the Covenant places an obligation upon a State party to respect and to ensure rights 'to all individuals within its territory and subject to its jurisdiction', but it does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it.[74]

Therefore, even measures on foreign soil which do not violate the sovereignty of a foreign state may be prohibited because they violate the human rights of an individual.[75]

6 Conclusion

In international law discourse on cyber attacks, there has been much focus on the threshold for the use of force. Cyber attacks or intrusions which do not amount to the use of force, have often been held to be unproblematic. As I have argued here, however, such intrusions will often constitute illegal interventions into the sovereignty of another state, or constitute violations of human rights.

Nevertheless, it is not completely clear how the usual rules of international law should be understood in this space. As mentioned, states have not been very helpful in clarifying these issues. They have not agreed to negotiate a new convention or other form of legal instruments, they rarely speak about international law and cyberspace with any precision -- so we have very little *opinio juris*, and they are often silent of those incidents which do occur -- so we have very little public state practice.

For sure, the old principles and rules of international law apply to cyberspace, too. The lack of a new convention is therefore not an excuse for not trying to

---

[73] Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004), paragraphs 3, 6 & 10. Hence, I do not agree with Forcese in this respect; cf C Forcese, 'Spies Without Borders: International Law and Intelligence Collection', 5 *J. Nat'l Sec. L. Pol'y* (2011) *179*, 207.

[74] Sergio Euben Lopez Burgos v. Uruguay, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981). See also

[75] R. v. Hape, 2007 SCC 26 (CanLII), (2007) 2 SCR 292, para 101. <http://canlii.ca/t/1rq5n> retrieved on 2013-10-18.

comply with these rules. Nevertheless, there is a pressing need for international bodies to clarify these rules, in the form of new conventions or less formal documents. We need to know of what terms like 'use of force', 'jurisdiction' or 'intervention' mean in cyberspace.[76] And we need to know if governments may invade our privacy. In that process, commentators on international law should play an important role.

[76] See also Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' (2013) 18 *Journal of Conflict and Security Law* 331, 350.