The Fourth Biennial Conference of the Asian Society of International Law
Delhi, 14-16 November, 2013

Intervention in national and private cyber space and international law

Presentation for the panel International Law and Cyberspace

Pål Wrange

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

The NSA affair has raised the issue of integrity in cyber space on the international agenda. According to the reports, the US National Security Agency has been evesdropping on both private and public communications in foreign countries.[1] Even though this has sparked a bit of a debate between international lawyers as to the lawfulness of these activities,[2] up until now, international legal doctrine has not had very much to say on such matters.

This paper will argue that intrusion in national cyberspace 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 is a which I have arrived at from the point of view of a generalist[3] through the application of general international law.[4]

---

[1] See "The NSA files", the Guardian, http://www.theguardian.com/world/the-nsa-files, accessed on 22 November, 2013.

[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.

[3] Although I have been involved with cyber issues now and then 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.

[4] Some more special regulations relevant to telecommunications adopted through the ITU (International Telecommmunications Union) may also be applicable, but they are not fully covered by this article.

1 Introduction

The topic of this paper is cyber intrusions into foreign cyberspace conducted by a state or under the control of state. This topic touches upon two protected values, namely sovereignty and human rights. I will start with state sovereignty, and discuss both law enforcement and espionage. Towards the end I will deal with human rights.

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. It is the territory that effectively determines the population, and the most important delimitation of the government's legitimate power is the territory – territorial jurisdiction. This territorial basis for political governance has been put in question by increased travel and migration, and governments now exercise at least some aspects of jurisdiction over considerable numbers of nationals abroad.

However, this complication is minor compared to those caused by Internet, which changes power relations among actors.[5]

Even though governments are increasingly taking control over their national cyberspaces, and the principle of territoriality provides that a state has jurisdiction over servers and nodes within its recognized borders,[6] the communication between servers and computers is routed in international webs mostly operated by private networks, which are not controlled by any one government,[7] and many virtual national assets are stored in servers. Perhaps most importantly, national assets in cyber space – public and private – can more or less easily be surveyed, affected or even controlled through cyber operations

[5] Cf JS NYE JR, CYBER POWER (2010), Harvard Kennedy School,Belfer Center for Science and International Affairs, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA522626 (last visited Nov 28, 2012).

[6] J Trachtman, *Global cyberterrorism, jurisdiction, and international organization*, GRADY, M.'THE LAW ECON. CYBERSECURITY 10 (2006), ftp://24.139.223.85/Public/Tesis_2011/legal_etchics/Perceptions2/others/globalcyberterrorim.pdf (last visited Nov 12, 2013). But cf JE Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 AFL REV. 43, 64 (2009), http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/airfor64&section=5 (last visited Nov 28, 2012).

[7] 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 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.

from foreign states, and in particular a few very technologically advanced ones, as I will exemplify. This has led some observers to suggest that the Internet is beyond the sovereignty of governments,[8] or even a new dimension, not subject to the same regulation as other spheres of human activities.[9]

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. Therefore, this paper will proceed from the axiom that the Internet and other computer networks are part of physical reality. 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 this summer in a report from a broadly representative group of 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 …

---

[8] 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 visited Oct 13, 2013).

[9] 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 visited Nov 12, 2013).

[10] On the possibilities of "renationalization" of the Internet, see C Engel, *The Role of Law in the Governance of the Internet*, INT. REV. LAW COMPUT. TECHNOL.1-16, 8 (2006); and E Tikk, *Comprehensive legal approach to cyber security*, 102 (2011), http://dspace.utlib.ee/dspace/handle/10062/17914 (last visited Oct 13, 2013).

[11] See WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19,9-10 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012),

[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 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), p 9. http://scholar.google.se/scholar?q=%22INTERNATIONAL+STRATEGY++FOR+CYBERSPACE%22&btnG=&hl=sv&as_sdt=0%2C5#1 (last visited 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.

> 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."

Nevertheless, it is very true that the situation is far from clear. *B

2 Sovereignty

So, the starting point must be that states exercise sovereignty over their respective cyberspaces, *mutatis mutandis*. However, states have many reasons to also take measures in foreign cyberspace. Some of these reasons are legitimate, like investigations of and responses to crimes, while others may be more dubious, like intelligence or sabotage. A state could for instance probe information on private computers, manipulate bank accounts, provide false information, interrupt the functioning of critical information infrastructure or create a break-down in the financial system.

Legally speaking some such acts may amount to armed attacks (warfare), illegal intervention, or legal countermeasures, depending on how they are characterized, 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 such acts might amount to the use of force, as is now a growing consensus among international lawyers.[14] As to what amounts to the use of force under Article 2(4) of the UN Charter, writers agree 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

[14] See Tallinn Manual, op cit, pp 46 et sseq.

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.

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 some 1000 centrifuges in the Iranian nuclear program.[15] Some would think of this as an act of force, but others disagree. Says one noted commentator: "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 not produce destructive consequences analogous to a kinetic military attack."

For many commentators, the discussion stops here. If an act does not constitute the use of force, it appears to be more or less unproblematic. However, many of these acts which do not constitute the use of force, like espionage may constitute illegal intervention or interference, and there has been much less debate on which acts constitute other forms of illegal intervention or interference.

2.1 Intervention, countermeasures and self-help

As Mary Ellen O'Connel reminds us, that "[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."[16]

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

[15] See, i.a., David P. Fidler, Revelations Concerning Cybersecurity, Recent Developments and Revelations Concerning Cybersecurity and Cyberspace : Implications for International Law, ASIL Insight 16 (2012).

[16] Mary Ellen O'Connell, *Cyber Mania*, *in* INTERNATIONAL LAW: MEETING SUMMARY: CYBER SECURITY AND INTERNATIONAL LAW 3, 6 (Mary Ellen O'Connell, Louise Arimatsu, & Elizabeth Wilmshurst eds., 2012).

> sovereignty. These actions can be authorized only by the territorial state."[17]

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."[18]

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. For instance, search of a home is illegal for a private person, and is thus prohibited.[19] And this applies also to various acts done in cyberspace, as I will argue shortly.

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 provide 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."

In this context it is important to note that a state may be responsible for acts performed by individuals, if these individuals are directed or controlled by a state or if the state in question adopts those acts as its own.[20] Furthermore, a state has the duty "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[21]

---

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

[18] Maziar Jamnejad & Michael Wood, *The Principle of Non-intervention*, 22 LEIDEN J. INT. LAW 345, 372 (2009).

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

[20] 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."

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

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".[22] However, there is no general mandate to take self-help measures. I will return to this issue in section 2.3.

2.2 *Intervention in national cyberspace in general*

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, i.e., international law limits they 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.[23]

This is confirmed by other writers.[24] However, there is controversy as to if intrusions that do not create any lasting harm are included. According to some writers, damage is irrelevant, whereas others find that only intrusions that cause material harm constitute illegal interventions.[25]

Kommentar [PW1]:

Kommentar [PW2]:

Kommentar [PW3]:

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, that is illegal, even if no physical harm has occurred. That must surely

---

[22] Article 25 of the ILC Draft Articles (footnote 20) 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.

[23] WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19, 11 & 12 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last visited Oct 13, 2013).

[24] C Forcese, *Spies Without Borders: International Law and Intelligence Collection*, J. NAT'L SEC. L. POL'Y 179, 201 (2011). See also T Tuukkanen, *Sovereignty in the Cyber Domain*, *in* THE FOG OF CYBER DEFENCE 37 (Jari Rantapelkonen & Mirva Salminen eds., 2013), http://www.academia.edu/download/30888836/The_Fog_of_Cyber_Defence_NDU_2013.pdf#page=38 (last visited Oct 13, 2013)..

[25] WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19, 11, 12 & 16 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last visited Oct 13, 2013).

apply also to servers or computers, and I have certainly seen no evidence of international customary or treaty law that would indicate and exception for searches on ICT machinery/gear. Under the Council of Europe's Budapest Convention on Cybercrime – which has been ratified also by 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 it 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.[26] This also seems to be the position taken by for instance US domestic law enforcement agencies.[27] Furthermore, the Convention has provisions on co-operation for the combat of these crimes and on extradition.[28]

2.3 Measures against terrorism and other forms of crime

Hence, the logical conclusion is that the general prohibition of intervention applies also in cyber space. Two fields of action where such intrusions may occur are the fight against crime and counterterrorism. This may involve different kinds of measures: investigations and prosecutions for crimes which have already occurred; enforcement of a judgment or a court order; a "hack-back" and investigation or interdiction of cyber-attacks in real time; deterring counter-strikes; and intelligence-collection in order to prevent crimes and terrorism. Some of these measures may damage hardware and software in other countries, but even more of them will constitute unauthorized intrusions in computers and servers or interfere with computer traffic.

Many such measures are covered by various international conventions against transnational crime and terrorism. While these conventions do not allow unauthorized interventions into the jurisdictions of other states, they do mandate states to cooperate with one another, as does the Council of Europe's Convention

---

[26] AM Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. LJ 425, 433 (2003). See also convention Art 32 of the Budapest Convention; Convention on Cybercrime, Council of Europe, ETS No 185, available at www.coe.org.

[27] See also SW Brenner & JJ Schwerha IV, *Transnational evidence gathering and local prosecution of international cybercrime*, XX J. MARSHALL J. COMPUT. INFO. L. 347–395, 386-388 (2001). However, for differences between the more "liberal" US approach and that of other states, see Ray August, *International Cyber-Jurisdiction: A Comparative Analysis*, 39 AM. BUS. LAW J. 531–573, 561-564 (2002).

[28] 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*, 27 BERKELEY J. INT. LAW 192, 223 (2009).

on Cybercrime.[29] 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.

It is sometimes argued that operations that take place from locations outside the target country are not illegal.[30] 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. 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.[31] 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 intervention.

The conclusion so far is that there are quite strong – though not clearly defined – limitations to what one state may do within the cyber space of another state. This, however, does not mean that a state which has been injured by attacks emanating from another state is entirely without recourse to legal means to react against attacks. I have already mentioned that a state may take countermeasures against another state which is violating international law. However, there are certain conditions, for instance that the purpose must be to "induce that State to comply with its obligations".[32] 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, in order to compel that state to cease the attack.[33]

---

[29] See footnote 26.

[30] J Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, UNIV. CHICAGO LEG. FORUM (2001), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732 (last visited Nov 28, 2012).

[31] See also August 535. Finns inte I medeley

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

[33] Unless other rule of international law would legalize Stuxnet, which I doubt

However, several of the most famous incidents, like Estonia 2007 and Georgia 2008,[34] have been difficult to attribute directly to a state. A state that harbors and actively assists terrorists or other criminals is legally responsible. [35] If the 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.[36] The duty "not to allow knowingly its territory to be used for acts contrary to the rights of other States" includes both the duty to investigate and prosecute, in cooperation with the target state, and a measure of active prevention.[37] A state is not responsible, however, if it could not know and if it could not prevent. It is unclear to what extent a state is supposed to survey its cyberspace.[38] Furthermore, the question is if this applies only to the hardware from which the attack is launched, or also to any lines through which the attack may be routed.[39]

However, 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

---

[34] E Tikk, *Comprehensive legal approach to cyber security*, 42-43 (2011), http://dspace.utlib.ee/dspace/handle/10062/17914 (last visited Oct 13, 2013).

[35] See Rule 11, the Tallinn Manual, note **Fel! Bokmärket är inte definierat.**. Cf also note 39.

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

[37] WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19, 16 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last visited Oct 13, 2013)..

[38] 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."

[39] 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." 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.

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."[40] This is clearly to take things too far, but there is some room for the invocation of necessity, as has been mentioned above.

In this context, it is necessary to mention the problem of attribution. It is generally very difficult to attribute a cyberattack to a particular subject in real time. This, of course, makes it difficult to determine what actions are appropriate and legal. However, this problem does not leave the state completely without opptions. Says Eneken Tikk:

> "[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."[41]

2.4 Espionage

Espionage, or secret intelligence, is to obtain information "covertly—that is, without the consent of the State that controls the information."[42] 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."[43] 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.

---

[40] SJ Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT. LAW 192, 237-238 (2009), http://works.bepress.com/scott_shackelford/5/ (last visited Nov 28, 2012).

[41] E Tikk, *Comprehensive legal approach to cyber security*, 105 (2011), http://dspace.utlib.ee/dspace/handle/10062/17914 (last visited Oct 13, 2013).

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

[43] www.freedictionary.com.

However, espionage may also involve unauthorized intrusion into servers including the collection of private and secret data. In May last year, 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."[44]

Doctrine used to be divided between the view that espionage is not regulated and the view that it is illegal, the latter view most forcefully argued by Quincy Wright.[45] In particular lately, some writers – notably quite a few American commentators – argue that espionage is legal under international law (in spite of being prohibited by domestic law),[46] and that there is therefore no obstacle to committing espionage over the Internet.[47] Those who make that argument essentially say that espionage is not prohibited and that there is a universal custom to engage in espionage. 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, as mentioned above.

---

[44] Flame_malware, Wikipedia, visited 13 November 2013.

[45] Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 11 (Roland Stanger ed., 1962). See C Forcese, *Spies Without Borders: International Law and Intelligence Collection*, J. NAT'L SEC. L. POL'Y 179, 202 (2011). See also S Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, MICHIGAN J. INT. LAW 1071, 1074-75 (2006).

[46] WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19, 11 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last visited Oct 13, 2013).xxx

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

See also the review in C Forcese, *Spies Without Borders: International Law and Intelligence Collection*, J. NAT'L SEC. L. POL'Y 179, 204 (2011).

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

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.[48] However, there are several counterarguments, and the most important one is that this is based on a complete misunderstanding of what constitutes customary law. (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. On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof.[49] In fact, 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.

I therefore conclude that espionage that involves crimes against the domestic law of the target state generally constitute illegal interventions into the sovereignty of that state.[50] This, of course, applies even more to covert operations or preparations for war that involve destruction of or tampering with data.

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.[51]

---

[48] 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." WH von Heinegg, *Legal implications of territorial sovereignty in cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFL ICT 7–19, 16 (C Czosseck, R Ottis, & K Ziolkowski eds., 2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243962 (last visited Oct 13, 2013).

[49] "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*, J. NAT'L SEC. L. POL'Y (2011). Tuukkanen is undecided. T Tuukkanen, *Sovereignty in the Cyber Domain*, *in* THE FOG OF CYBER DEFENCE 37, 43 (Jari Rantapelkonen & Mirva Salminen eds., 2013), http://www.academia.edu/download/30888836/The_Fog_of_Cyber_Defence_NDU_2013.pdf#page=38 (last visited Oct 13, 2013).

[50] There may be exceptions, for instance if the relevant domestic law of the target state is in violation of human rights.

[51] "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

3 Human rights

States are not the only entities with rights under international law. Individuals also have rights, relevant to cyber intrusions. One such 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 cyber space – 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, for instance, terrorism, will have to respect this right.

This paper 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:

> 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 also to cyberspace. This means that an intrusion by a state into a protected server in another state or an interception of messages in outer space may constitute not only a violation of that other state's sovereignty, but also a violation of the human rights of another person. It is important to note that Article 17 does not prohibit all interference – interference shall not be arbitrary or unlawful -- suggesting 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

---

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 179, 208 (2011)

> 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. Searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment. …

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 states that want to act differently need to make a convincing counterargument.[52]

It may be argued that the ICCPR does not protect individuals situated beyond the territory of the state taking measures in cyberspace.[53] 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, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

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:

---

[52] 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).

[53] See for example 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. CF for instance 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. 329, 357-358 (2004).

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 whether the state is in charge. The Human Rights Committee has confirmed this dichotomy and confirmed that the convention has extraterritorial application, though not in exactly the same terms.[54] Therefore, even measures which do not violate the sovereignty of a foreign state may be prohibited because they violate the human rights of an individual.[55]

This means that measures in foreign cyberspace that can be justified by consent, necessity or as countermeasures can still be in violation of international law of they violate human rights. 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). It is important in this context to remember 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. It must also be justified under Article 17 of the ICCPR. 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."

4 Conclusion

In international law discourse on cyber attacks, there has been much focus on the threshold for the use of force. Cyber attacks or intrustions which do not amount to the use of force, that is, violations of Article 2(4), have often been held to be

[54] 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 179, 207 (2011).

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

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 area. Unfortunately, states have not been very helpful in clarifying these issues. States 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.

The old principles and rules of international law apply to cyber space, too. The lack of a new convention is therefore not an excuse for not trying to 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 clarifications of what terms like "use of force", jurisdiction or intervention mean in cyberspace. We also need global procedures to enhance cooperation between states --- and I believe that the Budapest Convention provides at least a part of the answer – as well for confidence building.

The discussion needs to continue, and it needs to involve as many stakeholders as possible, in objective and professional discussions that proceed on both legitimate state interests and on legitimate interests of individuals.