Update paper:

Global mass surveillance in relation to military espionage

Legal committee

Harvard Model United Nations India 2017

Introduction:

While there are domestic laws, for instance, the United States' Privacy Act of 1974, and international laws such as Article 17 of the International Covenant on Civil and Political Rights which both guarantee civilians the right to privacy and protection from unlawful inspection of their communications[1, 2], there is nothing to regulate inter-governmental surveillance as there is no international legislature that codifies specific rules governing global mass surveillance and espionage.

Some jurists have indeed argued that one government gathering intelligence on another could be viewed as an unfriendly act seeing as it does violate the spirit of Article 2 of the United Nations Charter[3] which aside from guaranteeing every member nation the right to sovereign equality, urges countries to refrain from the use of force in all forms, against the sovereignty or political independence of any state[4].

Nevertheless, several nations such as those party to the Five Eyes agreement have suggested that the use of mass surveillance, especially in a military context is integral to ensure the safety of their citizens even if the threat to that safety is not imminent.

Therefore, this paper will focus on not only helping delegates gain a better comprehension of global mass surveillance in relation to military espionage but also on aiding delegates in their ability to analyse the legalities of the matter.

Defining military espionage:

Military espionage otherwise referred to as military intelligence is information gathered by a government on a foreign military with a specific focus on their operations, ideology and official policy[5]. Said foreign military can be another country's armed forces or non-state actors such as militias and terrorist organisations.

After the 2013-2014 Edward Snowden leaks, a great emphasis was and still is placed on domestic surveillance, political espionage, and diplomatic surveillance. However, little focus was given to the mass intelligence programmes conducted by governments on foreign militaries making this a key issue under the agenda.

Aside from cases of governments monitoring the activity of terrorist groups, some instances of mass surveillance systems being used for the purpose of military espionage include reports of the NSA monitoring computers in Hong Kong and Mainland China some of which were military systems[7], the GCHQ purportedly gathering years' worth of intelligence on the Israeli army[8] and finally, the Australian Secret Intelligence Service allegedly intercepting the communications of former military head and security minister of Indonesia, Widodo Adi Sucipto[9].

Naturally, cases of global mass surveillance such as the aforementioned ones remain unverified seeing as the only corroborating evidence is the Snowden leaks. Nonetheless, the very idea that countries are using mass surveillance systems to spy on foreign militaries could be concerning to some members of the international community.

The need for global mass surveillance in relation to military espionage:

Several government officials such as former President Barrack Obama, senior members of the United States Congress and former UK Chancellor of the Exchequer, George Osborne have emphasised the importance of the work done by the NSA and GCHQ asserting that mass surveillance is in the interest of national security, not just of their own nation but of all members of the international community, primarily due to the increasing number of global terror threats.[10, 11]

In fact, the former chairman of the US House Permanent Select Committee on Intelligence, Rep. Mike Rogers stated that the NSA's programmes had recently stopped 54 terrorist attacks in the US and even the EU. Similar claims were made by former NSA director, General Keith Alexander[12]. Unfortunately, little evidence has been published to support these claims, and in fact, some evidence contradicts these statements as discussed later.

Nevertheless, one might argue that even the potential for threat whether imminent or not is enough of a reason to conduct surveillance on foreign armed forces as it may uncover even a prospective threat which could at some point be beneficial to the safety and security of a nation. For example, according to the Snowden leaks, the NSA gathered intelligence on Huawei, a Chinese

telecommunications giant they believed was working with the Chinese government and that they also believed posed a significant threat to the US government's cyber-security[13].

Ramifications of global mass surveillance for military espionage:

A notable consequence of the Snowden leaks is the potentially irreparable damage done to the international community's diplomatic relations. For instance, after reports surfaced that the NSA intercepted German Chancellor Angela Merkel's mobile phone conversations[14], talks on matter dominated the following EU summit where there were detailed discussions on how such actions could undermine the trust held between allies[15].

In the context of this sub-topic, as mentioned in the introduction, the gathering of military intelligence could be seen as an infringement on a country's sovereignty and this is particularly problematic as it sets a bad precedent for the international community. To elaborate, several nations take cues from larger, more influential countries such as the United States and the United Kingdom meaning if these nations normalise the surveillance of foreign militaries, there is nothing to stop the rest of the international community from doing the same which as a result could threaten the very national security they are trying to protect.

Furthermore, the unintended legitimisation of military espionage creates significant room for abuse. For example, authoritarian regimes may abuse mass surveillance technologies by engaging in cyber warfare in order compromise the integrity of foreign armed forces and groups that oppose their rule[16]. Evidence for this has already emerged with a recent Privacy International investigative report claiming, for instance, that private companies have sold mass surveillance technologies to the governments of countries including Ethiopia, Bahrain and Libya, and are being used to target pro-democracy groups, among other targets[17].

Finally, a point often raised by privacy rights advocates is that mass surveillance on a foreign military may not be particularly effective in accomplishing what it sets out to do. In fact, a member of the United States' White House review panel for the NSA surveillance programme stated that there was not a single case of an attack by a terrorist organisation thwarted by mass surveillance systems[18],

which calls into question the necessity for governments to expend resources on a potentially nugatory process, especially given its apparent negative consequences.

Conclusion:

With no specific law to govern the issue, no state is legally liable for any wrongdoing when they engage in military espionage using mass surveillance systems. However, as mentioned in the introduction, it at the very least impinges on the spirit and foundations of diplomacy and international law. Therefore, the reality is, as per the status quo, military espionage through mass surveillance technology is neither legal nor illegal under international law leaving the matter in a rather ambiguous legal grey area. Some scholars argue that the matter is contextual[19] where if the benefits of a particular case of surveillance outweigh its limitations then it is more defensible than if it were the other way around.

To conclude, this paper has, as a matter of course, provided a superficial analysis of the matter which delegates must build on in order to ensure the best possible outcome. Countries that are opposed to military espionage and mass surveillance must formulate a comprehensive set of solutions to aid in the codification of an international law that holds violators accountable. Countries that are in favour of military espionage and mass surveillance need to construct a plan to offset the potential ramifications such as those discussed on the previous page; And finally, those that believe in a middle ground must come to a consensus on what aspects of the matter must be written into law and what aspects need to remain as they are.

Links for further reading:

1) http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1170&context=mjil
2) https://www.ilsa.org/jessup/jessup16/Batch%202/DeeksLegalFramework.pdf
3) http://remotecontrolproject.org/wp-content/uploads/2015/07/Mass-surveillance-briefing-paper.pdf
4) https://www.tni.org/files/download/state_of_surveillance_chapter.pdf

Bibliography:

[1] "Privacy Act of 1974." *The United States Department of Justice*. N.p., n.d. Web. 09 July 2017.
[2] "International Covenant on Civil and Political Rights." *OHCHR |ICCPR*. N.p., n.d. Web. 09 July 2017.
[3] Radsan, John, A. *The Unresolved Equation of Espionage and International Law*. N.p.: Michigan Journal of International Law, 2007. PDF. Pg.603
[4]"Charter of the United Nations." *United Nations*. United Nations, n.d. Web. 09 July 2017.
[5]"Military espionage." *Dictionary of Military and Associated Terms.* 2005. US Department of Defense 10 Jul. 2017
[6]"Edward Snowden: Leaks that exposed US spy programme." *BBC News*. BBC, 17 Jan. 2014. Web. 10 July 2017.
[7] Szoldra, Paul. "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks." *Business Insider*. Business Insider, 16 Sept. 2016. Web. 10 July 2017.
[8] Follorou, Jacques. "Britain has spent years spying on Israel's leaders." *Le Monde.fr*. Le Monde, 08 Dec. 2016. Web. 10 July 2017.
[9]MacAskill, Ewen, and Lenore Taylor. "Australia's spy agencies targeted Indonesian president's mobile phone." *The Guardian*. Guardian News and Media, 17 Nov. 2013. Web. 10 July 2017.
[10]"Chancellor's speech to GCHQ on cyber security." *Chancellor's speech to GCHQ on cyber security - GOV.UK*. N.p., n.d. Web. 10 July 2017.
[11]"Do NSA's Bulk Surveillance Programs Stop Terrorists?" *New America*. N.p., n.d. Web. 10 July 2017.
[12]Ibid.
[13] Szoldra, Paul. "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks." *Business Insider*. Business Insider, 16 Sept. 2016. Web. 10 July 2017.
[14] Sherwell, Philip. "Barack Obama 'approved tapping Angela Merkel's phone 3 years ago'." *The Telegraph*. Telegraph Media Group, 27 Oct. 2013. Web. 10 July 2017.
[15] "Edward Snowden: Leaks that exposed US spy programme." *BBC News*. BBC, 17 Jan. 2014. Web. 10 July 2017.
[16]Kersley, Esther. *Mass surveillance: security by 'remote control' - consequences and effectiveness*. N.p.: REMOTE CONTROL, Aug. 2015. PDF. Pg.4
[17] Ibid.
[18] Isikoff, Michael. "NSA program stopped no terror attacks, says White House panel member." *NBCNews.com*. NBCUniversal News Group, 20 Dec. 2013. Web. 10 July 2017.
[19] Radsan, John, A. *The Unresolved Equation of Espionage and International Law*. N.p.: Michigan Journal of International Law, 2007. PDF. Pg.603