Forum: Disarmament and International Security Committee

Issue: National Security Leaks

Student Officer: Nefeli Ioannou

Position: Co-Chair

PERSONAL INTRODUCTION

Dear Delegates,

My name is Nefeli Ioannou and I will serve as the co-chair of the Disarmament and International Security Committee, or the First Committee of the General Assembly, for this Conference. This will be my second time chairing, as I approach the end of three memorable years of participation in MUN. It will also be my last MUN Conference, at least as a high school student, and I really look forward to spending it with you!

I am a senior student at HAEF Athens College and I take great interest in the topics of Disarmament, since disarmament is the core goal of the United Nations, in its pursuit to achieve global peace and international security. I have participated in Disarmament Committees as a delegate in a number of conferences and so I know how challenging a committee it can be. Especially with the topics that have been chosen for this year, I am certain that we will have a heated but productive debate.

As the co-chair of GA1, I am here to make sure that every single one of you gets the most out of this Conference. This is why I would like all of you to know that I will always be available for any help you might need during your preparation period and, of course, during the Conference itself. In that respect, this study guide aims at getting you familiarised with the key issues that revolve around the rather complicated and certainly exhilarating topic of National Security Leaks. It will constitute, I hope, a good starting point for your research which should, however, extend to other sources as well.

I'm really looking forward to meeting and working with all of you in the Conference and, in the meantime, feel free to contact me.

Best Regards,

Nefeli Ioannou

INTRODUCTION

The fear of terrorism following the attacks of 9/11 and the digital revolution that led to an explosion in cell phone and internet use have marked the launch of a new era in the long history of government surveillance, the so called "Golden Age of Surveillance".

The revelations made by the former National Security Agency contractor Edward Snowden to the anti-secrecy group Wiki Leaks regarding the intelligence collection mechanisms of NSA and other Western intelligence agencies have caused public outrage, mainly because of the unprecedented scale and depth of the surveillance programs. Whereas coordinated intelligence activities have helped countries effectively tackle problems of the modern world such as the combat of terrorism and various other criminal activities, there has always been an inherent conflict between upholding fundamental human rights and fostering national security. Although not the first case of government surveillance uncovered, the Snowden affair has added new dimensions in the ongoing public policy debate as to whether national security concerns, allegedly protected by intelligence agencies, can bypass the democratic and judicial oversight system of a country, infringe on national sovereignty of other countries and violate fundamental human rights and civil liberties such as the right to privacy and the freedom of expression. Despite the existence of divergent views, an international consensus is building up among governments, international organizations, institutions, civic organizations and citizens in favour of a balance between national security and civil liberties. In the words of the President of the United States Barack Obama "we have to set up a system of checks and balances. We should not sacrifice freedom in order to have security".

DEFINITION OF KEY TERMS

National Security Leaks

The term national security leaks refers to revelations to the public (mainly through the press) of classified information regarding top-secret government surveillance programs operated by intelligence agencies as a means of counteracting serious internal or external threats to national security.

National Security Threats

Threats against national security include:

- **Terrorism**, carried out by international and domestic terrorist groups;
- **Espionage**, with a number of foreign states seeking to acquire sensitive information and technologies;
- **Cyber**, used by hostile actors to conduct espionage operations or launch damaging computer network attacks;
- **Proliferation of weapons of mass destruction**, which threatens international peace and stability. (source: MI5 Security Service)

Intelligence

Intelligence is the lawful process of collecting, evaluating and analysing information needed to make informed decisions related to law enforcement, national security, and defence and foreign policy objectives. The Intelligence capability of a country in the modern post cold war era, realized through the network of its intelligent services, is considered an indispensable prerequisite to satisfying the vast information requirements of a country with respect to the adoption and implementation of foreign and defence policy.

A wide range of information falls within the spectrum of information targeted by intelligence services in their activities. This information includes:

-Military Information: This type of information is required in order to plan a country's military strategy and organize its armed forces, referring mainly to defence systems and resources, technical information on weapons, location of troops, defence plans and strategies. This type of information is of primary interest to enemies in war time as well as to terrorist organizations. They also provides useful data in the context of peacetime negotiations of arms control agreements

-Industrial Information: This type of secret information usually refers to strategic sectors of a country's economy such as communication technologies, computers, genetics, aviation, laser and optics. They also have a great impact on the conduct of diplomacy.

-Political and Economic Information: This category of information entails critical details regarding policy priorities, negotiation positions and stances, secret economic decisions.

In that respect, a clear distinction should be made between espionage and intelligence. Whenever the gathering, evaluation and process of the information is conducted by **the official employees of a state's respective agency** operating openly as such and through the use of lawful means such as publicly available and other open sources (national archives, media, international agreements, diplomatic relations and information exchange), then we are talking about an intelligence operation justified for a variety of national security and international stability considerations.

Espionage

Intelligence is usually confused with espionage which is the process whereby a government, an organization or an individual seeks to obtain information which is not publicly available and without the permission of the information holder. Contrary to intelligence, espionage usually involves the employment of unethical or illegal means resulting in the infringement of fundamental human rights such as the right to privacy and international law principles. In many cases, however, it is really difficult to draw the line between a lawful intelligence operation and a covert espionage activity.

BACKGROUND INFORMATION

Historical Overview

The history of intelligence and surveillance can be traced back in the early stages of state organization. Countries and governments have always striven through more or less developed forms of intelligence to get access to and gather not publicly available, classified information through covert means. Surveillance and espionage have been credited with winning wars, forestalling revolutions, provoking them in certain cases, protecting the world from terrorist attacks and in general exercising a far reaching influence on historical development.

Writing almost 2500 years ago, the Chinese military theorist Sun Tzu (flourished 6th century BC) stressed the importance of intelligence in his book *The Art of War* (circa 500 *BC*): *"Enlightened rulers and good generals who are able to obtain intelligent agents as spies are certain for great achievements".*

The invention of the first electronic media, the telegraph, as early as in the late 19th century marks the beginning of the era of **electronic surveillance** in the current, prevailing form of interception of communications. **Wiretapping** – tapping the telegraph wire anywhere along its wire to listen to a message-became the first electronic surveillance operation widely used during the American Civil War, when both the Union and the Confederacy tapped into each other's telegraph lines and copied messages. The practice was condemned by many US states which introduced relevant legislation, whereas individuals resorted to codes and ciphers in an effort to maintain their privacy.

Mass surveillance entered a new phase **during World Wars I and II** where a number of electronic devices developed by major electronics companies, such as the Magnetophon developed by AEG in the Nazi Germany, were used to record and monitor cable transmissions both by states in a national security context as well as by police and detectives in crime investigation. In the aftermath of World War II, the US became involved in the first large scale, massively intrusive global surveillance program, under the name **Operation Shamrock**, which continued until 1975. The program operated in parallel with **Project Minaret**, secretly intercepting and reading millions of telegraph messages between US citizens and international sources, especially those considered "unreliable," such as civil rights leaders and antiwar protesters, and opposition figures such as politicians, diplomats, businessmen, trades union leaders, non-government organizations like Amnesty International, and senior officials of the Catholic Church. The program was terminated in 1975 following the report of the **Church Committee**, set up by the Senate to investigate illegal activities carried out by US intelligence organizations. The Church Committee's final report called Shamrock "probably the largest government interception program affecting Americans ever undertaken." [CHURCH COMMITTEE, 4/23/1976] The Church Committee Report and the subsequent termination of the program came down to history as the first chapter in the still ongoing debate as to the relationship between national security and civil liberties and led to the introduction of a stricter judicial oversight mechanism such as the Foreign Intelligence Surveillance Act (FISA) enacted in 1978. Since 1978, the NSA and other US intelligence agencies have been restrained in their wiretapping and surveillance of US citizens by the provisions of FISA.

The new Era in Electronic Surveillance

The digital revolution and the explosion in the use of Internet and mobile phones have marked the beginning of a new era in the data collection mechanisms and practices of the intelligence agencies. In the information age we are living in, the advances of digital technology have made available to intelligence services a wide range of electronic surveillance (photographic, sensing, Iand detection) devices and other techniques, contributing to the development of super powerful intelligence collection mechanisms targeting governments and individuals and linked to foreign policy goals. We have therefore segued into the electronic surveillance era. Traditionally, intelligence agencies have intercepted international communication by focusing on satellites and microwave towers. However, nowadays satellite interception accounts only for a small part of internet traffic. Most of it travels on fiber-optic cables. This is the area where intelligence agencies are focusing. More specifically, intelligence agencies, and predominantly the NSA in cooperation with its British counterpart GCHQ, have been able to tap into the network of fiber optic cables that carry the world's phone calls and internet traffic, store huge volumes of sensitive personal data drawn from these cables for up to 30 days and then process and analyse this information. Data collected through such means is a powerful tool in the hands of international agencies when aimed at specific targets. Surveillance programs have helped intelligence agencies in the war on terror, allowing them to discover new techniques used by the terrorists to avoid security checks as well as to identify terrorists planning atrocities. They have been also used successfully in the field of cyber defence and against networks engaged in grave forms of international crime such as human trafficking, drug trade and child exploitation.

The legitimacy of these operations, however, has been seriously questioned as is evident from the worldwide outrage caused by the Snowden Affair.

Major Electronic Surveillance Programs

Prism: Prism is a clandestine mass electronic surveillance and data collecting program operated by the National Security Agency of the USA. Subject to permission granted by the secretive Foreign Intelligence Surveillance Court, the NSA and the US government are allowed to request data on specific targets from some of the USA's biggest technology companies like Google, Apple, Yahoo, Facebook, Microsoft, and also have direct access to such information from the servers of these companies. Access to Prism classified information is also allowed to the UK's spy agency GCHQ.

Tempora: Tempora is a mass-interception network operated by the UK's GCHQ spy agency for huge amounts of data flowing in and out of the UK. This network is based on tapping fibre-optic cables and using it to create a vast "internet buffer". The system falls within GCHQ's greater surveillance goal to "Master the Internet" and relies on the involvement of a number of telecommunications companies (BT, Verizon Business, Vodafone Cable, Global Crossing, Viatel and Interoute)

Upstream: Upstream refers to a number of similar to Tempora bulk-intercept programs carried out by the NSA. Collection of data relies on intercepting huge fibre-optic communications cables with the assistance of US telecommunication companies. According to recent revelations all the metadata (sender, recipient, time) collected through Upstream

and Prism are stored by the NSA in a database system called MARINA for 12 months. Storage of the content of the communications has not been verified.

Cracking cryptography: Both the NSA and GCHQ operate ultra-secret programs aimed at undermining encryption, the technology which underpins the safety and security of the Internet , including email accounts, commerce, banking and official records. These ultra-secret programs are codenamed by both agencies after their countries' respective civil war battles: BULLRUN for the NSA and EDGEHILL for GCHQ.

Overview of Nine Major National Security Leaks in US History

-Pentagon Papers: June 1971, the Nixon Administration

The case: Daniela Ellsberg, a US military analyst employed by RAND Corporation, a nonprofit global policy think tank, released to the media (New York Times, Washington Post and 17 other newspapers) a top secret 7000 pages of U.S. decision making in Vietnam, known as the Pentagon Papers.

The Charges: He was charged with three charges under the 1917 Espionage Act (Receiving, Communicating and Retaining National Defence Document)

Case Outcome: Dismissed

His Statement: *"I felt that as an American citizen, as a responsible citizen, I could no longer cooperate in concealing this information from the American public."*

- Samuel Morison: October 1984, Ronald Reagan Administration

The case: Samuel Morison, an American intelligence professional, leaked confidential satellite images of Soviet nuclear-powered aircraft carriers to a military defense magazine.

The Charges: Charged under the 1917 Espionage Act with Communicating and Retaining National Defense Documents

Case Outcome: Convicted to two years imprisonment – Pardoned by President Clinton in 2001, despite opposition by the CIA

His Statement: *"If the American people knew what the Soviets were doing, they would increase the defense budget."*

- Lawrence Franklin: May 2005, George W. Bush Administration

The case: Lawrence Franklin, a former United States Department of Defense employee, passed classified documents regarding U.S. policy towards Iran to the American Israel Public Affairs Committee (AIPAC), who in turn provided the information to Israel.

The Charges: Charged under the 1917 Espionage Act with Communicating and Retaining National Defense Documents

Case Outcome: Convicted to thirteen years imprisonment

-Thomas Drake: April 2010 | Barack Obama Administration

The case: Thomas Drake, a senior executive of the NSA, revealed in a media interview a series of details regarding waste, fraud and abuse at the NSA, after his complaints had been repeatedly dismissed

The Charges: Charged under the Espionage Act

Case Outcome: Government dropped all espionage charges. Convicted only for misusing the agency's computer system

His Statement: *"I did what I did because I am rooted in the faith that my duty was to the American people."*

-Shamai Leibowitz: May 2010, Barack Obama Administration

The case: Shamai Leibowitz, a Hebrew linguist working for FBI, passed to a blogger, classified FBI wiretaps with discussions of Israeli diplomats about Iran
The Charges: Charged under the Espionage Act for Disclosure of Classified Information
Case Outcome: Convicted

-Bradley Manning: May 2010, Barack Obama Administration
The case: Pfc. Bradley Manning was charged with multiple violations of the Espionage Act after disclosing more than 700,000 classified state department cables and government documents to WikiLeaks.
The Charges: Charged with 22 offenses, including several under the Espionage Act
Case Outcome: Sentenced to 35 years in prison and dishonourably discharged

-Jeffrey Sterling: December 2010, Barack Obama Administration

The case: The case is directly related to Operation Merlin and has been the most important case in the context of national security leaks, up until the outbreak of the Snowden Scandal. Jeffrey Sterling, a former CIA officer was prosecuted for revealing details about Operation Merlin -an alleged covert operation under the Clinton Administration to provide Iran with a flawed design for building a nuclear weapon in order to delay the alleged Iranian nuclear weapons program. Operation Merlin, one of the most spectacular screw-ups in the history of the agency, was the theme of the book
" State of War" of the two-time Pulitzer winner, New York Times journalist Tom Riesen, to whom Sterling allegedly passed the information. A full excerpt of his book was published in The Guardian in May 2006. Riesen has never named Sterling as one of his sources and has consistently refused to reveal his sources. Following Sterling's prosecution, prosecutors have been trying for years to get Risen testify at Sterling's leak trial which has been on hold since 2011 largely because of legal disputes over whether Risen could be forced to testify. On January 15th this year, Riesen was finally cleared from having to testify, removing the risk that he could have faced jail time if he refused to testify**.**
The Charges: Charged under the Espionage Act for Unauthorized Disclosure and Unlawful Detention of National Defense Information
Case Outcome: The trial is currently in progress-No verdict yet reached

-John Kiriakou: January 2012, Barack Obama

The case: John Kiriakou, a former CIA analyst and counterterrorism officer, was charged with disclosing to a reporter the identity of a covert CIA agent who had been involved in a CIA's "enhanced" interrogation program.
The Charges: Charged under the Espionage Act as well as under the Intelligence Identities Protection Act

Case Outcome: Convicted solely on the count of offenses under the Intelligence Identities Act
His Statement: *"I believe my case was about torture, not about leaking. I'm right on the torture issue, the administration is wrong, and I'm just going to carry that with me."*

-Edward Snowden: June 2013, Barack Obama Administration
The case: Edward Snowden, a former CIA employee and NSA subcontractor, became the source of the worst leak in US intelligence history and the controversial center of public attention when in May 2013 he released to the media documents allegedly detailing the inner workings of various extensive internet and phone surveillance programs operated by NSA and other intelligence agencies. According to these revelations millions of calls, mails and other communication worldwide were intercepted by the NSA, assisted by the "Five Eyes" intelligence -sharing group, of Australia, Canada, New Zealand, UK and the US. The scandal broke up in June 2013 with a report on The Guardian disclosing a secret FISA court order directing telecommunications company Verizon to hand over all its telephone data to the NSA on an "ongoing daily basis". The report was followed by revelations in both the Washington Post and The Guardian regarding NSA surveillance program known as Prism, operated jointly with British intelligence agency GCHQ, which enabled direct tapping into the servers of nine internet companies including Facebook, Google, Microsoft and Yahoo. Snowden was identified by The Guardian as the source of the leaks at his own request and after he had fled USA. Snowden and his media associates continued to leak top secret, classified information regarding various surveillance programs, including tapping fiber optic cables carrying worldwide communications (Tempora), eavesdropping on mobile phones of 38 world leaders (including German Chancellor Angela Merkel and Brazilian President Dilma Rousseff), spying on internet networks of EU and UN offices and foreign countries embassies and many other snooping operations of an unprecedented scale and extent
The Charges: Edward Snowden was charged with many offenses under the 1917 Espionage Act including Unauthorized Communication of National Defence Information and Wilful Communication of Classified Communications Intelligence Information to an Unauthorized Person. Initially fled to Hong Kong, he has been granted temporary asylum by Russia, where he currently resides. His passport has been revoked and American officials ask for his extradition to the USA.
Case Outcome: Ongoing
His Statement: "*Being called a traitor by Dick Cheney is the highest honor you can give an American, and the more panicked talk we hear from people like him ... the better off we all are".*

Public Policy Debate Issue: National Security vs. Civil Liberties

The issue of electronic surveillance and communication interception, especially in the digital era, has been put squarely on the international agenda following the revelations made by the former NSA contractor Edward Snowden. The Snowden files disclosed in the most explosive way the ability of the intelligence agencies to access information stored by major US technology companies, often without individual warrants, to intercept data from the fibre-optic cables which make up the backbone of global phone and internet networks and also to threaten the effectiveness of the security systems of major communication and financial networks such as internet, commercial transactions and financial services.

Almost one and a half year after its outbreak, the Snowden Scandal and the public policy debate it has sparked remains a highly controversial and enduring topic. It will always arise when the domains of national security and public safety collide with the citizens' right to privacy, the public's right to know and the principles of freedom of expression. For many, the topic is one of the most important topics of our time, nothing less than the defence of democracy in the digital age. For others, there is an inherent conflict of interests and balancing them equates with an effort to square the circle. Don't intrude but keep me safe. How to square such a circle? US President Barack Obama himself, while consenting to the need for a thorough reform in the US surveillance policies and NSA practices, he went on to state that "*we do not have to sacrifice freedom in order to have security. My job is both to protect our people and to protect the American way of living which includes privacy. We have to make decisions on how much classified information and how much covert activities we as a society are willing to tolerate. The public needs to have an assurance that there are checks and balances in place"*.

The tragic terrorist events in Paris and the failure accusations against the French intelligence have raised again the voices of concern of privacy advocates that these attacks might be used as an excuse for a further expansion of the already extensive surveillance powers enjoyed by intelligence agencies worldwide. At the same time they have been invoked by many supporters of the need for a retooled intelligence enterprise that could "connect the dots" and keep us safe in the wake of the wildest phase of the war on terror. In the words of a former NSA executive*: "In order to find the needle in the haystack, you need access to the whole haystack"*

Another important aspect in the context of national security leaks is the role of the press in upholding individual rights and civil liberties. Individual journalists entangled in controversial leak stories have always defended their public duty to hold governments accountable for any violation of fundamental human rights and democratic processes and have striven in order to gain access to public records, meetings and court rooms and disclose the acquired information. There are many cases, however, where journalists have been accused of exploiting the treasure trove of information secured through their cooperation with whistleblowers or otherwise for their own personal benefit rather than the common good. In the Snowden case, there have been many speculations regarding lucrative business deals with publishers and movie producers signed by some of the journalists Edward Snowden has partnered with. The media involvement of multibillionaires like the eBay founder Pierre Omidyar in launching a new media organization, First Look Media, dedicated to"fearless and adversarial" journalism and in funding the so called crypto insurgency aimed at the US intelligence apparatus is being viewed with increasing scepticism by many traditional advocates of press independence.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

Almost every single country in the world operates a secretive arm of government consisting of intelligent agencies of varying degree of organization, staffing, sophistication and impact on world affairs. At an international scale and for the purposes of the current study, we will focus on the six biggest intelligence agencies.

The end of the Cold War Era has not led to world peace and eradication of conflicts around the world. The world dominance of the USA is being challenged by the rise in power of new global players, economic competition is becoming fiercer in the context of a crisis-prone world economy, historical hostilities are being rekindled and extremist movements are on the surge worldwide. All the above reasons have kept the intelligence agencies of many countries more than busy and have furthered the expansion of communications interception and electronic espionage. The most important intelligence agencies are the following:

Central Intelligence Agency- CIA and National Security Agency- NSA

Country: USA

The US Intelligence System constitutes an elaborate complex of some dozen separate independent or quasi-independent intelligence organizations, each with a specific role and a carefully defined area of expertise and responsibilities. The Central Intelligence Agency CIA continues to sit on the top of this complex, with its Director being the president's principal intelligence adviser, responsible for coordinating all the separate intelligence units. The biggest of the country's myriad intelligence organizations is the National Security Agency/Central Security Service(NSA),the USA's signals intelligence agency as well as the phone and internet interception specialist of the USA, which is also responsible for code breaking .It has a strict focus on overseas, rather than domestic, surveillance. The role of the CIA, and more recently of the NSA, has been questioned on a number of occasions, following the disillusionment of the Vietnam War, the Watergate scandal, numerous accusations for illegitimate interventions and support to authoritarian regimes. As a result of extensive media disclosures and investigations by presidential commissions and congressional committees, new guidelines for secret operations were adopted and a new structure for executive and legislative supervision established. The controversy however remains and is becoming more intense in the information age, following the recent revelations.

Government Communications Headquarters- GCHQ

Country: United Kingdom

GCHQ is UK's official security and intelligence organization, working in close cooperation with the British Government and subjected to Parliamentary and judicial control. GCHQ forms an integral part of the British intelligence heritage, which dates back to the two World Wars and the Cold War. CHQ is a secret organization and its very existence was not officially admitted until 1983.

Foreign Intelligence Service- SVR

Country: Russia

SVR is carrying on Russia's formidable spying tradition, which dates back to the czarist-era Cheka and the once omnipotent KGB of the Soviet Union. Although its officially declared area of expertise is to counter terrorism and protect Russia's commercial interests, SVR is heavily involved in international espionage and consolidation of domestic political power.

Ministry of State Security- MSS

Country: China

MSS is close in structure to the old Soviet KGB and is responsible for both domestic security and foreign espionage. The high tech industries and the military technology of the United

States are the main focus of its overseas activities. MSS is also believed to be leading China's aggressive espionage efforts on cyberspace. Since 2007, the governments of the USA, Britain and Germany have been making continuous allegations against China for attempting to hack and hacking into their respective Departments of Defence databases. Chinese espionage is different than Western espionage, in that it does not rely solely on purposefully recruited and trained agents, but views every individual and every little piece of information as a potential intelligent asset, making it extremely difficult to detect the scope of its operations.

Research and Analysis Wing- RAW
Country: India

India's notoriously secretive agency was founded in 1985 as an indispensable arm of the Indian government's strategy against Pakistan .Since then it has developed to one of the strongest intelligent agencies, with its activities expanding to Pakistan, Sri Lanka, Nepal, Bangladesh, and elsewhere. Its main objective remains the destabilization of Pakistan and to this end it is particularly active in supporting independence movements in Bangladesh, whereas it has been also accused by Pakistani authorities for terrorist attacks in their country and for infiltration by U.S. and Chinese assets.

Inter-Services Intelligence- ISI
Country: Pakistan

ISI is the counterpart of RAW in Pakistan, aimed at undermining India's stability by spreading anti-Indian propaganda, backing separatist movements inside India and assisting terrorist attacks. ISI is also considered to be cooperating with the USA and its allies in the global war on terror fighting, al Qaeda, the Taliban and other Islamist extremists inside Pakistan, although it has been also accused of offering aid to selective terrorist group abroad. ISI is also described as a state within state in Pakistan, escaping any kind of democratic or judicial oversight with respect to domestic politics.

Mossad
Country: Israel

Mossad, the most important of Israel's major intelligence agencies, carries out foreign espionage and covert political and paramilitary operations against the country's Arab neighbors and Palestinian organizations. It has the reputation of an extremely effective organization, being credited with a number of successful operations for the protection of the Israeli interests such as the apprehension of Adolf Eichmann in Argentina, the execution of the killers of Israeli athletes at the 1972 Olympics, and the rescue of Israeli hostages in the Entebbe incident. In the late 20th and early 21st centuries, the Mossad was criticized for its treatment of detainees, many of whom were allegedly tortured and killed while in custody, and for its efforts to assassinate Palestinian political leaders.

Internet and Tech Companies

The Internet giants Apple, Facebook, Google, Microsoft, Yahoo, Twitter, AOL and Paltalk as well as major US and UK telecommunications companies have been also identified as key actors in the world spying story, having allegedly provided to US intelligence agencies backdoor or direct access to their vast trove of information stored in their data centre (e-mails, videos, online chats, photos and search queries) via the Prism Program. Tech

companies are required to hand over data in response to a legitimate request under the provisions of the Foreign Information Surveillance Act (FISA) or an individual court order. They have no obligation however to provide the government with full, indiscriminate access to their servers. Tech companies have fought aggressively against orders they do not consider legitimate and have repeatedly advocated greater government transparency, publishing themselves detailed transparency reports detailing government requests for information, in all cases they are allowed to do so.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

General Assembly Resolution 68/167 on the "Right to Privacy in the Digital Era".

Resolution, initiated by Brazil and Germany following the Snowden revelations and voted unanimously by the 193 UN members in December 2013, expresses deep concern at the negative impact that surveillance and interception of communications may have on human rights and calls on a curb of supernormal surveillance of communications. The General Assembly affirms that the rights held by people offline must also be protected online and calls upon all States to respect and protect the right to privacy in digital communication. It also "calls on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasizes the need for States to ensure the full and effective implementation of their obligations under international human rights law".

UN Group of Governmental Experts (GGE):

Following the submission of two consensus reports in 2010 and 2013 a new UN Group of Governmental Experts (GGE) was authorized with an expanded mandate on issues related to the state use of information and communication technologies and their compatibility with international law. The report of the Group's findings is scheduled to be discussed the 70th session of the General Assembly in 2015.

International Covenant on Civil and Political Rights

Ratified to date by 167 States the Convention provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, or to unlawful attacks on his or her honour and reputation. It further states that "Everyone has the right to the protection of the law against such interference or attacks."

PREVIOUS ATTEMPTS TO SOLVE THE PROBLEM

The Snowden Files and the extensive media coverage of their disclosure have raised worldwide serious concerns about growing domestic surveillance, the scale of global monitoring, the trustworthiness of the technology sector, the ability of the state and the intelligence agencies to keep their information secure and the quality of the laws and the oversight mechanisms in keeping the agencies in check. They have sparked an intensive public debate regarding the balance between the two colliding imperatives, namely national security and civil liberties.

Despite the intensity of the public debate, however, even the most explosive disclosures have not caused any big rupture in great powers world politics. They have simply confirmed what was already known, or at least suspected, among highly ranked intelligence agencies executives, security analysts and knowledgeable observers: that great powers politics include cyber-attacks against not only rivals but also allies, bugging institutions, monitoring global internet communication and compromising key communications software and encryption systems designed to protect online privacy and security.

At the domestic level, espionage activities are considered to be illegal under national law and almost all states have enacted legislation criminalizing the conduct of such activities. Mass surveillance activities undertaken by intelligence agencies, as the ones described above, are authorized under specific legislation setting strict conditions thereof such as the FISA Amendment Act of 2008 and the Patriot Act in the USA and the Regulation of Investigatory Powers Act (RIPA) in the UK. Revelations on GCHQ and NSA activities however have given rise to many concerns, raised particularly by law makers in the USA, as to whether the actual interpretation and implementation of the law by the intelligence agencies complies with the original intent of the legislature when enacting the relevant rules. Moreover, the operation of the intelligence agencies is being supervised and controlled domestically by democratic and judicial oversight mechanisms such as the Foreign Intelligence Surveillance Court, operating in secret, and the Senate Intelligence Committee in the USA and the British Parliament's Intelligence and Security Committee in the UK. In the wake of the Snowden affair and in response to widespread public and congressional pressure the Obama Administration has been forced to consider reforms to the operations of US intelligence organizations and to declassify hundreds of pages of rulings from the federal court.

At the international level, a very strong reaction is coming from the world's internet security community. Intelligence agencies are being accused by prominent academics, researchers, corporate executives and many civil organizations of "subverting" the internet into a multi-layered , robust surveillance platform, damaging the reputation of the US tech companies and seriously questioning the moral authority of the US as the steward of the internet. Civil organizations such as the Electronic Frontier Group and Scientists' Joint Declarations have also warned for the overall world security implications since the recent revelations regarding the Western intelligence agencies surveillance programs are in fact legitimizing internet abuses by Russia, China, Iran and totalitarian regimes and called for the need to redesign security standards and establish new means of Internet governance, promoting transparency, oversight and accountability and thereby restoring interstate trust and cooperation.

Moreover, all intelligence agencies are called upon to comply with the provisions of the European Convention of Human Rights as to their obligation to respect the right to privacy in the conduct of their operations. Individual citizens, private corporations as well as state entities have the right to mount legal action against intelligence agencies for violation of the above right in the International Court of Justice, as with a legal case against GCHQ by three UK privacy groups.

Cyber spying and US control of such a globally valuable resource have given rise to international efforts sponsored by China and Russia to put the stewardship of Internet to the hands of the United Nations. Such efforts have been resisted by the USA and the majority of the international community.

Traditional international law, however, remains remarkably oblivious to the peacetime practice of espionage. Major international treaties fail to address the delicate issue of espionage and its potentially detrimental impact on interstate relations or confine any reference to espionage to a mere definition of what constituted a spy and a description of the legal consequences in the unfortunate event of capture. There has been no major international initiative following the breaking of the Snowden affair aiming at the signing of a new Treaty, despite the fact that it was universally acknowledged that the disclosed surveillance operations conflict with a state's obligations under human rights and international law as they infringe upon the national sovereignty of other states and the right to privacy of individuals. Growing interstate suspicion has led great powers to focus their efforts on crafting offensive and defensive capacities in cyberspace and other surveillance areas instead of fostering an international cooperation aimed at negotiating and agreeing to a universally binding regulatory framework governing cyberspace security and electronic surveillance. The truth is however that in that respect, they tend to further enhance interstate suspicion, especially between historical rivals such as the USA and Russia or emerging fierce competitors such as the USA and China.

The importance of such an international cooperation is highlighted in instances where coordinated and joint intelligence activities, justified on grounds related to national and international security considerations, have proved to be extremely successful in foiling terrorist operations through the penetration of international terrorist organizations as well as in thwarting major international crimes such as international drug traffic.

POSSIBLE SOLUTIONS

At the international and multilateral level, in the light of the confidence destroying revelations of the Snowden Affair, all states should be encouraged to promote and sustain within the framework of UN and other international institutions a constructive dialogue with a view to maintaining international stability and security and upholding fundamental human rights, both offline and online. In the context of this dialogue emphasis should be placed on the adoption of confidence building measures that will provide incentives for cooperation on shared threats (international terrorism and organized crime) and create disincentives for states to engage in competitive espionage. Similar efforts should be undertaken at a bilateral or regional level through the signing of agreements that will help increase transparency, predictability and trust (codes of ethics on sharing information intelligence).

At the domestic level, there is a growing need for new legislation aimed at further strengthening the adequacy of the oversight infrastructure and the protection of the individual's rights. These legislative reforms should always be balanced against the legitimate pursuits of domestic and international surveillance as well as against the perils of opaque or questionable leaks.

A significant role is also assigned to the scientific community in the development of new technologies to counteract the surveillance mechanisms of state intelligence. Equally important is the role of the mass media in disclosing state abuses and helping build public and institutional pressure. Finally, we should never lose sight of the importance of the individual responsibility of each and every citizen in upholding his own rights and defending democracy against visible and invisible enemies.

BIBLIOGRAPHY

- https://www.ciaonet.org/cbr/cbr00/video/cbr_ctd/cbr_ctd_22a.pdf
- http://alumnos.cva.itesm.mx/unctec/wp-content/uploads/2014/02/SC-2014-Handbook.pdf
- http://rt.com/news/un-resolution-worldwide-surveillance-476/
- http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/
- https://www.mi5.gov.uk/home/the-threats/espionage/how-do-spies-operate.html
- http://diplomacy.unyouth.org.nz/uploads/c59405a3a34fe3b6bd0bec25addbb904.pdf
- http://autocww2.colorado.edu/~toldy3/E64ContentFiles/PoliticsAndGovernment/espionage.htm
- http://strategicscience.org/the-difference-between-intelligence-and-espionage/
- http://www.leadershiponline.co.za/articles/electronic-espionage-saga-7845.html
- http://descrier.co.uk/news/world/where-has-the-snowden-affair-left-international-diplomacy/
- http://www.foreignaffairs.com/articles/140155/henry-farrell-and-martha-finnemore/the-end-of-hypocrisy
- http://www.globalissues.org/article/802/surveillance-state
- http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all&_r=0
- http://www.foreignpolicy.com/articles/2008/01/20/the_list_the_worlds_top_spy_agencies?wp_login_redirect=0
- http://www.bloomberg.com/news/2012-12-10/u-s-intelligence-agencies-see-a-different-world-in-2030.html
- http://www.theguardian.com/world/the-nsa-files
- http://www.theguardian.com/law/2013/sep/17/fisa-court-bulk-phone-records-collection
- http://www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security
- http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-interne
- http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy

- http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
- https://archive.org/stream/essaysonespionag00stanrich#page/n45/mode/2up
- http://www.un.org/Docs/journal/En/20131105e.pdf
- http://dash.harvard.edu/bitstream/handle/1/10900863/Benkler.pdf?sequence=1
- http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf
- http://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1001&context=political_science_hontheses
- http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet
- http://www.pbs.org/newshour/rundown/edward-snowden/
- http://www.pbs.org/newshour/spc/multimedia/espionage/
- http://www.globalresearch.ca/video-secrets-for-sale-and-the-snowden-affair-the-greenwaldomidyarnsa-connection/5364393
- http://www.theguardian.com/commentisfree/2015/jan/09/guardian-view-surveillance-after-paris
- http://www.worldaffairsjournal.org/article/what-it-takes-defense-nsa
- http://nymag.com/daily/intelligencer/2014/10/pierre-omidyar-first-look-media.html