LGSMUN IX

[DISEC]

TOPIC AREA A

Foreign Military Bases; A Threat to National Sovereignty

Introduction to the Committee

The Disarmament and International Security Committee (DISEC), also known as the First Committee, is one of the six main committees of the United Nations General Assembly. It addresses disarmament and international security matters in the light of the general principles of cooperation to the maintenance of international peace and security, in order to prevent the disruption of armed conflict and the heightening of tensions in the international system. Since the past decade, the committee has been focusing on issues of nuclear non-proliferation, small arms illicit traffic and regional militarization.

As a subsidiary organ of the General Assembly, the DISEC is entitled to present its recommendations over the issues under its consideration to a plenary meeting of the Assembly, usually in the form of draft resolutions and decisions. Through this mechanism, the First Committee has been the primary origin of legal initiatives that led to important international treaties and conventions, such as the Treaty of Non-Proliferation of Nuclear Weapons of 1968 and the Comprehensive Nuclear Test Ban Treaty of 1996.

Each Member State of the United Nations is represented by one delegate in this committee and decisions on draft resolutions and recommendations are approved on a two-thirds majority basis, turning the DISEC into a broad and inclusive platform for the debate of pertinent issues concerning the maintenance of international peace and security.

Outline of the Problem

Ever since the development of the modern city-state in Ancient Greece, the concept of military bases outside a nation's territory has been established. Foreign military bases were at their peak during the Cold War. Ever since the end of the Cold War, there has been a decrease in the number of overseas military developments, particularly so from the Soviet side. However the number of foreign US bases has not just stayed the same, but increased with the advent of the Gulf Wars from the early 1990s. The Russian Federation has 25 military bases abroad, mostly located in the ex-Soviet republics of Eastern Europe. France and Britain's overseas military bases are mostly the remnants of past colonies. Undoubtedly the largest network of military bases across the world is that of the USA. The US Department of Defence defines foreign military bases in the following terms: "The term 'military installation' means a base, camp, post, station, yard, centre, homeport facility or any ship, or any other activity under the jurisdiction of a department, agency, or other instrumentality of the Department of Defense, including a leased facility, except that such term shall not include any facility used primarily for civil works, rivers and harbor projects, or flood control projects. An installation is a grouping of facilities, located in the same vicinity, which support the same Air

Force operations." Foreign military bases are controversial for their negative effects on host countries, and for the way that they contravene the international norm of sovereignty. This topic seeks to focus on how the spread of foreign military bases across the world has affected host nations and what the best international framework or unified strategy to deal with the problems posed by such bases would be.

History of the Problem

Foreign military bases, particularly those of the United States, have historically been acquired during, or after, wars. Take for example the US base in Guantanamo, Cuba, which was set up after the Spanish American War. The treaty entitling the United States to this base states that the US control is permanent as long as nominal annual payments are made and may be relinquished only by the mutual consent of both the US and Cuba. Obviously, this does not take into account the views of both the Cuban government and populace, which have on many occasions vehemently demonstrated their hostility to a US base on their soil. Besides the Guantanamo Bay base, many of the United States' bases around the world were set up as result of wars ranging from the Korean War to the present day conflict in Afghanistan.

1898	USA captures Guantanamo Bay
1977	France deploys approximately 3000 troops in Djibouti as per Defense Agreement.
March 1990	US National Security Strategy published. Quotes include "[W]e are inescapably the leader, the connecting link in a global alliance of democracies."
January 1991	US-led coalition launches "Operation Desert Storm"
1991	US deployments continue after the war has ended, with 17000-24000 US troops in the Persian Gulf at any point in time.
1991	Philippines announces to the USA that it must withdraw from the Subic Bay naval base by the end of the 1992
June 1999	UNSC Resolution 1244 legitimizes NATO to establish a Kosovo Force overseas base in Kosovo.
2002	2 teenage girls killed by US soldiers in South Korea. Soldiers return to the USA without a trial.
October 2002	UN urges US to withdraw from the Puerto Rican island of Vieques. USA withdraws in 2003
April 2004	Cuba tables a UN resolution regarding Guantanamo Bay.
June 2004	International Committee of the Red Cross inspects Guantanamo Bay and rules treatment of suspects tantamount to torture
September 2004	UN Resolution 1559 calls on Syria to withdraw its overseas military base from Lebanon and stop intervening in Lebanese politics.
May 2006	UN Committee against Torture condemns the violation of the UN Convention Against torture in the Guantanamo Base and calls on the US to close this overseas military base.
November 2007	Czech demonstrations against a military base; the US and Czech

	Republic plan to set up near Prague for radar for an anti-missile system that will be based in Poland
January 2008	Citing UNSC Resolution 1778 the European Union launches its overseas military base in eastern Chad and the north-east of the Central African Republic.
January 2009	Barack Obama announced the suspension of the Guantanamo Military Commission for 120 days, and declared that it would be shut down within a year.
January 2013	The Guantanamo Bay Base is still open.

Contentious Issues

The lack of an international framework or consensus on how to deal with the myriad issues raised by the presence of foreign military bases in sovereign states raise several contentious issues that will undoubtedly cause heated debate amongst delegates in the committee room.

Status of Force Agreements

A Status of Force Agreement (SOFA) is an agreement between a host country and a foreign nation stationing forces in that host country. The purpose of a SOFA is to lay down the rights, privileges and limits foreign personnel serving in a host country are subject to. Globalsecurity.org defines SOFAs as coming in three different forms. “These include administrative and technical staff status under the Vienna Convention on Diplomatic Privileges, commonly referred to as A and T status; a "mini" status-of-forces agreement, often used for a short-term presence, such as an exercise; and a full-blown, permanent status-of-forces agreement.” As such, a SOFA is not a mutual defence or security agreement, although it may be part of one. It instead lays down a mechanism for legally protecting the rights of foreign military personnel who are present in a host nation. Delegates are encouraged to research the various SOFA agreements between nations and the controversies stemming from them. There is no singular framework for a SOFA agreement. Each agreement differs from case to case as numerous factors must be taken into account; the current security arrangements and concerns, nature and duration of missions, sentiments of the local populace, and the credibility and rights of jurisdiction. The US has the highest of number of personnel posted across the globe. US SOFAs give provisions in criminal issues for U.S courts to have jurisdiction over crimes committed against other servicemen, or as part of their military duty. The Host Nation retains jurisdiction over other crimes. In principle this holds true; however there are examples of crimes which include murder, rape, thievery and even gross human rights violation where the perpetrators have walked free. A major issue is that most host nations have mixed feelings over the establishment and the influx of foreign military on their soil. Often demands for renegotiation and local pressure for calls of withdrawal cause political unrest. The difference in legal rights of a person within a host country and the personnel of the bases may differ, possibly resulting in miscarriages of justice. Another issue with agreements arises when there is blatant hypocrisy over the terms of SOFAs signed by a

nation. Taking the example of South Korea which has forces stationed in Kyrgyzstan, it has a SOFA which gives diplomatic immunity to its servicemen from being tried in Kyrgyz courts for any crime. This is far in excess of the privileges South Korea objects to in its SOFA with the US. However, according to US analysts, the numbers of accused tried in civilian courts is evident of the fact that SOFAs work.

NATO

North Atlantic Treaty Organization: is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defense whereby its member states agree to mutual defense in response to an attack by any external party. The admission of forces of a member state of the alliance remains subject to the consent of the receiving state. Legal Framework within NATO -The admission of forces of a member state of the alliance remains subject to the consent of the receiving state -This precondition has not been diminished in any way by the increased level of the defense integration that has taken place since the NAT entered into force.

Sovereignty of the Host Country

Foremost on the agenda when such a topic is bought into discussion, are the implications on the sovereignty of the host nation. But before these implications are explored, one must understand the concept of a sovereign nation. According to the UN, a sovereign state has an effective and independent government within a defined territory. Unfortunately there is no definition of what sovereignty implies as is evident in the words of famed International Law maker Lassa Oppenheim: “There exists perhaps no conception the meaning of which is more controversial than that of sovereignty. It is an indisputable fact that this conception, from the moment when it was introduced into political science until the present day, has never had a meaning which was universally agreed upon.” However there are certain markers generally agreed upon which highlight the sovereign status of a region, namely:

Absoluteness

A sovereign power has absolute sovereignty over the governed region only tampered by the rules and regulations decided upon within the country without influence of external actors. These include neighbouring nations or the much greyer influence exerted over various nations by intelligence agencies across the world.

Exclusivity

This denotes the exclusive right of a nation’s jurisdiction, specifically the degree to which decisions made by the state might be challenged or contradicted by another authority, International Law, or a foreign presence after which represent legal infringement on exclusivity.

De Jure and De Facto or Legal Sovereignty is concerned with the recognized right to exercise control over a territory. De facto or actual, sovereignty is concerned with whether control exists or not, which includes the cooperation and respect of the locals, control over the national

assets, means of security and ability to carry out various functions of governance.

Internal

This represents the relation between the governing body and its subjects, and by what right the governing body holds the power of governance.

External

This is concerned with the relations between a sovereign power and other states. External sovereignty is connected with questions of international law. For instance, when, if ever, is intervention by one country onto another's permissible?

Sovereign:

A government which exercises de facto administrative control over a country and is not subordinate to any other government in that country is a foreign sovereign state. - The Arantzazu Mendi, [1939] A.C. 256), Strouds Judicial Dictionary

Socioeconomic issues

The establishment of foreign military bases leaves a very distinct footmark on the socioeconomic, political and environmental assets of the host nation. To understand the impact these bases have one must look at the connection established in the book Imperial Footprint: America's Foreign Military bases, by Zoltan Grossman: "The environmental, political, and economic impact of these bases is enormous and, despite Pentagon claims that the bases simply provide security to the regions they are in, most of the world's people feel anything but reassured by this global reach. Some communities pay the highest price: their farmland taken for bases, their children neurologically damaged by military jet fuel in their water supplies, their neighbors imprisoned, tortured, and disappeared by the autocratic regimes that survive on U.S. military and political support given as a form of tacit rent for the bases. "Such acts can be seen as violations of the parameters set to measure the sovereignty of a state. The overreaching influence causes the weakening of defacto sovereignty within a nation as people's mistrust in the government grows because of the inaction to solve the problems as already stated. As already discussed in SOFAs, the right of jurisdiction may be violated even though stated otherwise in the SOFA which impedes the internal sovereign rights of a nation. Even the right of governance and of the populace to live in their locality can be violated as is evident by the tragedy of Diego Garcia, ostensibly a tiny British island-colony in the Indian Ocean. All of the island's residents were evicted in the 1960s so that it could be occupied by an enormous US base that has served as a lynchpin in every US Middle East invasion and occupation since that time. The residents were not provided with any compensation for this gross violation of de jure sovereignty.

Covert Operations

A covert operation is a military, intelligence or law enforcement operation carried out clandestinely and usually outside official channels. Such operations take place without the knowledge of any other parties except the ones sponsoring or carrying out the operations. Foreign bases play a vital role in such operations as they often serve as forward base of operations and localized intelligence cells reporting back to the foreign nation from the host country without fear of liability because of the immunities often granted in State of Force Agreements. Many infamous covert operations caused great controversy such as the training of rebels in Cuba for the Bay of Pigs invasion, or the training of Afghan rebels during the Soviet invasion of Afghanistan at known or hidden military bases at neighbouring countries. A more recent example is the May 2nd 2011 operation against Osama Bin Laden by US Navy Seals in Pakistan which was done without the knowledge of the Pakistani government; this raid was launched from one of the US bases near the Pakistani-Afghan border. Covert operations, in other countries neighbouring the host nation or even in the host nation is a contentious issue which represents one of the fundamental violations of the sovereignty of a nation and is often used by the Anti-Base movements as an argument in winning support for foreclosures of bases.

Aiding in Natural Disasters

In current times there is a growing trend for armed forces around the world to go beyond traditional warfare and take on humanitarian and development related tasks. The post-cold war repositioning is responsible for some of these factors; other reasons may include the professionalization of armed forces, the phasing out of draft and a greater investment in and management of each soldier's career pattern has begun a search for new roles as 'forces for good' or 'humanitarian warriors'. It also reflects moves towards more comprehensive approaches to security. So when a natural disaster strikes, not only the Armed Forces of the host country, but also the Visiting Forces, get activated into action. The International Disaster Recovery Association, (IDRA), has been helped during times of natural calamities by Armed Forces of countries around the world, especially by the United States which makes its military assets available for 24 disaster response. Countries like the USA have a stated policy of maintaining an active international role for its military. The fact that they maintain a number of military bases globally enables them to reach the affected countries very quickly. Similarly, during the Earthquake in Pakistan on October 8th, 2005, the Visiting Forces of the USA and NATO, already present in neighbouring country Afghanistan, at the request of the United Nations, were immediately activated and within hours, helicopters and other military assets and personnel were deployed to assist initially in search and rescue efforts, followed by medical and rehabilitation efforts. The responsibility of aiding a populace in case of a natural disaster lies with civilian institutions; however, foreign military involvement in disaster relief has increased over the past 40 years. This raises questions regarding the deployment, degree of

involvement and withdrawal of troops from the affected areas. The military is more adept to responding to disasters as they are readily trained to combat any contingency situation, and adapt rapidly to changing situations. The disaster relief provided by foreign military forces, is a two sided coin, on one hand it reduces the load on the disaster hit nation's civil and military response units. On the other hand though, such endeavours may often be used to further agendas, or establish a foothold in a region otherwise unavailable. The example of Haiti which suffered the devastating earthquake in 2010, easily demonstrates how a military presence can help further the humanitarian effort, and at the same time, present a reason for extended periods of stay of thousands of military personnel, and transference of military from assistance to supervisory roles in relief efforts. A foreign base in the disaster hit country has its advantages as an additional asset for disaster management and relief, but it also provides an opportunity for the foreign nation to gain access to areas of the host nation otherwise restricted. Therefore the delegates must come to a conclusion whether the benefits outweigh the cons in the overall scenario not just during times of crises.

Economics of Bases

The economic strains on the country owning bases in various nations increases exponentially as each new base is set up, the prime example of how much the cost can be, is United States of America with an annual spending of 1.9 Trillion dollars in 2008 on its foreign bases. However such bases often provide a boost to the economy of the host country, as it creates new opportunities for work, for example the construction of bases is often done by local construction contractors as to reduce the costs for the foreign nation. As long as the base exists it also creates a trade cycle for local business for various items. Besides the obvious, there is a huge economic input in terms of long term leasing and other support infrastructure provided to the foreign nation, and in some cases the host nation is paid a compensating amount as per the SOFAs made. Another economic impact which is often overlooked is in terms of security spending as is exemplified by the presence of US military in the Philippines, which averted the Chinese from laying claim to certain resource rich Islands. When the US army left, the Philippines Navy spending increased by nearly $6 Billion so as to maintain the previous strategic advantage. But there are cases where ideological/political differences result is negative impacts to the economy of the host nation, in terms of increased 27 unrest, violence and damages to property, or if the bases required the eviction and acquisition of prime lands resulting in the loss of real state capital, as in the example of Guam where two maps were compared, one showing the island's best fishing grounds, agricultural lands and drinking water, the other showed the location of US military bases; the maps were identical. It is difficult to gauge the economic impacts of foreign military bases across the globe as the impacts vary from nation to nation because of many contributing factors such as ideological differences, stability within the country, political standings, and history of the formation of bases. The delegates can clearly see that foreign bases

across Europe have a positive impact on the economy as compared to the negative economic reactions seen in Afghanistan, Pakistan, and Iraq etc. In looking at economic impacts one also needs to consider the implications on the input to the host nations GDP and local populace of the area in case of foreclosures of bases, Panama was able to recover from the foreclosures, but the same may not hold true in Afghanistan and Iraq.

CASE STUDIES

Afghanistan

Foreign military presence in Afghanistan has historical roots with consequences that last until today. During the Cold War, the state became a strategic area to the Soviet Union. In order to gain influence in Central Asia and spread the communist ideology, the USSR occupied the country in December 1979, as it had been asked by the leftist government that ruled the Democratic Republic of Afghanistan since 1978 (Barfield 2010). In that period, many insurgent groups named Mujahideen have come to oppose the soviet intervention. This opposition was in accordance with USA's interests of containing USSR influence. Therefore, the North-American government sent money and weapons to support the rebels, with the support of Pakistan and Saudi Arabia. It was also in this period that Taliban emerged as a political and religious movement against the soviet presence in Afghanistan. The conflict lasted almost ten years, ending with the soviet troop's withdrawal in February 1989 (Barfield 2010). After the USSR's departure, the communist government established in Afghanistan eventually fell, in 1992. From this moment on, a civil war started between the Mujahideen groups that fought the Soviets and the Taliban for the control of the country. After four years fighting, the Taliban finally broke into the capital Kabul and dominated about 90% of the region, then establishing the Islamic Emirate of Afghanistan (Barfield 2010).

The 9/11 attacks and the Afghanistan War

The Islamic Emirate of Afghanistan was a theocratic government against Western presence in the country. Due to its restrictive and radical policies, the Emirate has been international recognized only by Pakistan, Saudi Arabia and the United Arab Emirates (Barfield 2010). Even with the lack of international support, the Taliban's government was able to control the country until 2001, after the 9/11 attacks. Under George W. Bush's administration, the USA has blamed the Islamic militant organization, Al-Qaeda, for being responsible for terrorism practices and has accused Taliban of protecting and supporting the organization. It was the beginning of the War on Terror (Gall 2014). As retaliation, Washington unleashed the punitive Afghanistan War in October 2001, with US bombings in Afghan cities. The USA entered in the country under the claim that Osama Bin Laden, leader of Al-Qaeda, was hidden under Taliban's protection. In 2002, after the consolidation of the US presence in the region, Hamid Karzai became president of Afghanistan, under the support of Western powers, antiTaliban Afghan groups and the United Nations. With the end of the Taliban regime in the country, the USA

increased their influence by the establishment of military bases (Gall 2014).

Main Foreign Military Bases in Afghanistan

Afghanistan has until today a great number of foreign military bases in its territory. The USA is the country with more installations, but other Western powers, such as the United Kingdom and Germany, have military facilities in the region too. However, nowadays, the North Atlantic Treaty Organization (NATO) has the control of most remaining bases due to the International Security Assistance Force (ISAF), a NATO mission established by the UN Security Council in December 2001.

The main US air base in Afghan territory is Bagram Airfield. Originally built by the Soviet military during its occupation, this base situated in the north of Kabul can hold up to 10,000 troops and serves as a prison too. In Bagram there is a runway where bomber aircrafts can land as well as huge transport aircrafts (BBC News 2009). According to The State Newspaper, the US have invested about $200 million in Bagram's infrastructure, with $68 million used only in the runway modernizationThe two main airports in Afghanistan, Kabul International Airport and Kandahar International Airport, serve as air bases as well as Bagram Airfield. Both airports were expanded and modernized by the USA and NATO between 2007 and 2009 and now operate civilian and military flights. Their infrastructure includes operational and maintenance facilities and housing and administrative installations (BBC News 2009). Other bases also have a key role in US and NATO logistics. Camp Joyce, for example, located along the Pakistani border, represents a strategic position since the Taliban is present in Pakistan nowadays (ABC News 2010). Countries such as the UK and Germany still have their bases in Afghanistan as Camp Bastian, the main British installation, and Camp Holland, under German administration (ABC News 2010).

USA-Afghanistan Agreements

Shortly thereafter Operation Enduring Freedom – the official name of the US intervention operation –, the Taliban was ousted by north-American and allied forces and many security agreements were concluded with the new Afghan government (Manson 2012). The first diplomatic contact between the two countries in order to discuss the US presence in Afghan territory occurred in September 2002, through an exchange of notes. The north-American government called upon The Foreign Assistance Act of 19615 to legitimate its intervention (Manson 2012). According to this act, the USA could apply defense measures against internal and external aggression, including military assistance to friendly countries: The act authorizes the President to furnish military assistance on such terms and conditions as he may determine, to any friendly country or international organization, the assisting of which the President finds will strengthen the security of the United States and promote world peace and which is otherwise eligible to receive such assistance (Manson 2012, p.7). Another exchange of notes dated from 2003 was responsible for the accord on foreign personnel status. The US claimed for an agreement equivalent to that accorded under the Vienna

Convention on Diplomatic Relation of 1961. According to the Convention, the north-American were immune from criminal prosecution by Afghan authorities as well as were immune from civil jurisdictions (Manson 2012). In 2004, the Afghanistan and the USA signed an Acquisition and Crossservicing Agreement, responsible for providing logistic support, supplies and services to foreign militaries in the country (Manson 2012). In 2005, President Hamid Karzai and President Bush issued a joint declaration in which they elaborated prospects for a future agreement to help organize, train, equip and sustain Afghan security forces until the country has developed its own capacity. However, efforts to regulate the relationship between the two states have not progressed (Manson 2012). The situation of US presence in Afghanistan have remained the same until December 2010, when the USA, under Barack Obama's administration, announced that US forces would commence a transfer of security responsibility to the Afghan government in 2011, which would be concluded in the end of 2014. Still in 2011, the official Status of Force Agreement begun to be negotiated to guarantee that the presence of US forces in Afghan territory is temporary and that all troops must withdraw from the country after one year of the agreement (Manson 2012). 5 The Foreign Assistance Act of 1961 was an act enacted by US Congress. It was responsible for organize the US assistance programs abroad, including military and economic aid. According to this act, the US would intervene, through assistance programs, in countries which were political and economic unstable, in order to help reinforce democratic values and avoid human rights violations (Manson 2012). Disarmament and International Security Committee 102 Finally, in 2012, the US-Afghanistan Strategic Partnership Agreement was signed. It is a legally binding executive agreement that provides a framework for the future relationship between both countries (White House 2012). The document reaffirms the cooperation principle and the shared goal of defeating Al-Qaeda and implements mechanisms to support Afghanistan's social and economic development. In practice, the agreement is a diplomatic measure to reinforce the commitments made by the two nations. Nonetheless, it has not a security role and does not provide for technical and legal issues concerning the US presence in the country (White House 2012).

Japan

The most pressing issue concerning foreign military bases established in Japan is its most strategic territory, Okinawa. It is the Japanese southernmost province and is formed by 169 islands which are together known as Ryukyu Archipelago (Sarantakes 2000). During World War II, Okinawa was a key region due to its localization near Taiwan, South Korea, Philippines and China. Therefore, north-America's access and control of the Pacific Ocean were related with US presence in these islands. In this context, the USA has prepared an offensive action in April 1945, penetrating with its naval forces the Japanese waters (Sarantakes 2000). The Okinawa Battle ended in June 22, 1945 and, as a consequence, the US remained in the region since it. With the end of the Second Great War, Okinawa has become essential to the north-American post war system. The fear of the

return of Japanese aggressive expansionism and the need to contain the soviet influence in Asia has stimulated the USA to create a military infrastructure in the Archipelago to consolidate its presence there (Sarantakes 2000). Episodes such as the Korean War (1950-1953) and the Vietnam War (1956-1975) required a great number of combat and support units which were provided through Okinawa (Fuqua 2001). Okinawa was under north-American administration until 1972, when the islands were brought back under Japanese sovereignty. However, even today, about 20% of Okinawa's main island surface is occupied by US military installations (Fuqua 2001).

US-Japan Agreements

The bilateral relationship between the USA and Japan after the World War II officially has begun in 1952, with the San Francisco Peace Treaty. The document was responsible for formalizing the end of the war. Article 3 officially led Okinawa under US administration, applying the concept of residual sovereignty. According to this principle, the USA would take care of this Japanese territory but its inhabitants would retain Japanese citizenship. It was a strategy to deal with possible accusations of colonization practices by the USA (Fuqua 2001). It was in 1960 that the most important treaty concerning US-Japan relations was accorded. The Treaty of Mutual Cooperation and Security guaranteed the use of Japanese territory by US air, naval and land forces in order to contribute to the security of Japan and the maintenance of international peace and security in Asia (Manson 2010). According to Jacques Fuqua of Indiana University, the document has two key points:

(…) first, Japan and the United States will respond to an attack against either party within Japan's territory. Second, Japan will provide land for U.S. military installations in its dual mission to provide security for Japan and the "Far East."

The first point results from Article IX of Japan's "Peace Constitution" (the 1947 constitution) which renounces Japan's sovereign right to wage war as a means of settling disputes and provides the rationale for a U.S. military presence in Japan. As a result, U.S. forces, along with Japan's own Self-Defense Forces, satisfy Japan's security requirements. (Fuqua 2001). Alongside the Security Treaty, the USA and Japan signed, in 1960, their Status of Force Agreement, providing a separate agreement to govern the status of US armed forces in Japanese territory. This SOFA provides extraterritoriality to US members and requires cooperation between both states in criminal investigations (Manson 2010). Finally, in 2006, the USA, under Bush's administration, signed an agreement with Japanese government to relocate a US marine air station to a less populated part of Okinawa. The accord has received several critics of the Okinawans who have claimed for the end of US military presence in the region (Fackler 2010).

The Future of Okinawa

The foreign military presence in Okinawa has many local impacts. A great number of old installations are now in populated areas since the archipelago were urbanized in the last years.

Thus, the population has to live with the extreme noise that comes from air bases and with the pollution coming from the military complexes. The rape of 12 years-old girl by members of US armed forces, in 1995, also has contributed to mobilize people against the crimes committed by US service members (Fuqua 2001). In this sense, the agreement proposed by the USA in 2006, in order to decrease the number of troops in the region and to relocate US bases, was an attempt to reduce hostilities between Okinawans and north-American troops. However, it has resulted in many popular manifestations against military bases (Fackler 2010). In 2009, Yukio Hatoyama was elected as Prime-Minister of Japan, promising in his campaign that he would be against the guidelines provided by the accord proposed by the US. During his administration, Hatoyama was pressured by public opinion and, at the same time, by the desire to maintain Japan-USA relations. Thus, in 2010, he announced that he would not fulfill his main election promise and would proceed with the agreement (Fackler 2010). In the last years, popular manifestations have increased, asking for the end of the colonial policy practice by the US in Okinawa (Fackler 2010). The fact that, historically, the islands were integrated lately into the Japanese Empire and, therefore, do not share the same culture identity with the rest of Japan, not being seen as “truly Japanese”, explains one of the reasons why Japan’s government do not try to meet popular claims, not transferring the bases to the mainland (Fuqua 2001). The former US Secretary of State, Hilary Clinton, claimed that the alliance between USA and Japan is the pillar of Asia-Pacific’s security and that this partnership requires close cooperation and coordinated policies (Foreign Policy Bulletin 2010). Thus, according to Clinton, there will be bilateral negotiations to reduce US military presence’s impacts, but the close relationship has to be reaffirmed: Let me repeat what American officials I have said ever since President Eisenhower signed our treaty 50 years ago: The commitment of the United States to Japan’s security is unwavering. To ensure that our alliance is well positioned to adapt and respond to evolving challenges, we must bolster our diplomatic engagement and security arrangements and ensure that our military posture can continue to provide the security that has been so instrumental in the region’s stability for so long. We must do this while reducing the impact on local communities by American military bases, particularly in Okinawa. Our two governments drew up the realignment roadmap with these dual goals in mind, and we look to our Japanese allies and friends to follow through on their commitments (Foreign Policy Bulletin 2010). Given US strategic interests of projecting influence in Pacific as well as Okinawa’s dependence on Japanese governmental support, the situation is unlikely to radically change. However, it is essential that US military commanders work actively with the Japanese state to further reduce impacts and crimes against local citizens as well as in working to answer local issues and concerns within the broader framework of Okinawa’s reality (Fuqua 2001).

Ukraine

The discussion about foreign military bases in Ukraine cannot be dissociated from the Cold War period and Russia's presence and influences in that territory. In 1954, Nikita Khrushchev controversially "gifted" Crimea to Ukraine, in honor of the 300th anniversary of Russian-Ukrainian unity – action that did not have political consequences until the dissolution of the USSR (Weir 2014). An important issue Disarmament and International Security Committee 108 to ponder is that Ukraine has a very clear concern with its territorial integrity, where the function of the state is to maintain its territory (Ukraine 1996). The country is divided in 27 units, where the importance of two specific units, the Crimean Peninsula and Sevastopol, is crucial to understand how relations with Russia are established – those are regions with autonomy.

Past International Actions

Over the years the efforts of the international committee to address these contentious issues have met with failures, as the key actors have much to lose by the formation of an international binding framework to oversee the construction, maintenance and closure of bases. Including the legal grey areas and issues of diplomatic immunity of soldiers as discussed in the guide so far. However since 2003 various community campaigns resisting military bases have started to join forces to address the spread of military bases through an international campaign. It is now known as "The international network for the abolition of foreign military bases" or "No Bases Network". The first global conference was held in 2007 in Quito and Manta, Ecuador where the two main objectives were laid out: 28 1. To support the local and regional groups that are members of the Network by sharing information, developing joint strategies, and helping new campaigns to get on their feet. 2.To create space in international forums and at the UN for a critical debate both on the legality and necessity of foreign bases as a method of military domination and on the need for codes of conduct or 'setting minimal standards' for the use of existing bases. For this, the network actively engages with other international civil society networks and with intergovernmental forums, such as the NPT 2010 Review Process. The Network also lobbies 'host nation governments' and in Brussels and Washington.

Positions of Main Stakeholders:

The main division will be between countries who support the continuation of foreign military bases and those host countries who claim to be negatively affected by them.

NATO

The North Atlantic Treaty Organization (NATO) (compromised of the US, the UK, France and their allies) operates most of the foreign military bases of today. NATO views these installations as critical to upholding commitment for their allies, providing security in their treaty obligations and defending their foreign interests. Recently, these nations have tried to minimize the impact of individual bases by spreading out operations

over smaller, more numerous installations. The effects of Western bases play into the foreign policies of many countries worldwide. Since they operate many bases worldwide and are somewhat strategically dependent on them, NATO countries would not be amenable towards taking action to curb foreign military bases.

The United States, United Kingdom, France

The United States has the most foreign military bases, with much information about them in the previous sections. Many are controversial, however there are many examples of foreign military bases that are tolerated or accepted by host populations. Likewise, the UK, France, and Russia have a number of bases each around the world.

Russia

After the collapse of the Soviet Union and the end of the Cold War, the number of foreign military bases operated by Russia has seen a significant decline. However, it continues to maintain a presence in countries that were former Soviet Republics, such as Georgia, Azerbaijan and Turkmenistan. It also has signed agreements with other countries such as Vietnam and the Seychelles to expand its presence. As such, Russia would not like to see substantial legislation passed that limits the predominance of foreign military bases.

China

China opened its first military base in the Seychelles in 2011, signalling its growing naval presence in the Indian Ocean. Countries with expanding military presences, such as China, should think of their future needs in preparing their country position. Japan also has a single military base in Djibouti to help in the international efforts to combat piracy in the Horn of Africa.

Non-SCO Asian Nations

Foreign military bases in Asia are characterized by the large, permanent deployments of American troops in the territories of longstanding allies such as South Korea and Japan. These bases, along with others, heavily affect regional dynamics of countries such as China. They also have a significant impact on the local populace, and have been a source of internal debate in these countries. India also owns a foreign military base in nearby Tajikistan. Since they protect many of these nations, these nations would not be amenable to legislation curbing foreign military bases.

Africa

While no African countries operate bases outside of their territories, many countries host foreign military bases. Traditionally, there has been a great British and French military presence in Africa due to their colonial ties. Recently, the US has expanded their military installations in Africa, although not in quantities comparable to other regions. China has also expressed interest in setting up a base in Africa given its diplomatic reach in the region. Therefore, most African countries' positions depend on their populace's opinions on military bases. Have there been revolts in your African nation against foreign

military bases recently? If so, your African nation might be opposed to the prevalence of foreign military bases. Does your African nation benefit strategically from the presence of a foreign military base? If so, your African nation might welcome the prevalence of foreign military bases.

Germany:

Germany hosts one of the collections of US military personnel, who number almost 30,000 personnel over 15 bases. Whether these troops are a continued hangover from the Cold War or a necessary part of the NATO defence structure remains debatable. Poland has a similarly contentious relationship with Russia due to the presence of US troops.

Afghanistan:

Afghanistan hosts military bases for the United States and the United Kingdom. With the winding down of military operations, many in both the US and Afghanistan would like to see these bases drawn down. However, some have argued that they continue to support the stability of the country.

Questions A Resolution Must Answer:

• Should there be a binding international agreement on the regulation of foreign military bases? If so, what provisions should it contain?

• What is the acceptable diplomatic status of foreign troops stationed on military bases?

• What guidelines should there be in signing SOFA agreements to protect civilian populations and local cultures?

• Is there a solution to reducing the negative consequences of foreign military bases, especially concerning human rights?

Bibliography

http://cns.miis.edu/archive/wtc01/cabases.htm• http://www.atimes.com/atimes/Central_Asia/CEN-01-080114.html• http://russiamil.wordpress.com/2013/09/19/central-asian-military-and-security-forcesassessing-the-impact-of-foreign-assistance• http://csis.org/files/publication/130122_Mankoff_USCentralAsia_Web.pdf• http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/08spring/blank.pdf• http://www.worldcrunch.com/world-affairs/new-us-military-bases-in-central-asia-guesswho-isn-039-t-happy/kyrghizistan-moscow-afghanistan-militaryterrorism/c1s9425/#.UxYUfvmSxYQ• http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=167520• http://cns.miis.edu/npr/pdfs/101khan.pdf• http://books.google.com.pk/books?id=W-• http://books.google.com.pk/books?id=OKhChGd7nP0C•&pg=PA114&lpg=PA114&dq=d e-nuclearization+of+South+Asia&source=bl&ots=kAjLSa6OWP&sig=QS3ULXcUfni2GOIvCpkglfjm1Co&hl=en&sa=X&ei=MOUWU8GvFKKn0gG13oC4AQ&ved=0CEgQ6AEwBQ#v=

onepage&q=de-nuclearization%20of%20South%20Asia&f=false
http://en.wikipedia.org/wiki/South_Asia•
http://www.tandfonline.com/doi/abs/10.1080/00358538608453764?journalCode=ctr•
t20#.UxbRUM5xPX4
http://en.wikipedia.org/wiki/Southeast_Asian_Nuclear-Weapon-Free_Zone_Treaty•
http://pu.edu.pk/images/journal/pols/Currentissue-pdf/NAZIR%20HUSSAIN.pdf•
http://www.desistore.com/nuclear.html•
http://www.nti.org/treaties-and-regimes/southeast-asian-nuclear-weapon-free-zoneseanwfz-treaty-bangkok-treaty/•
http://www.dawn.com/news/661927/nuclear-deterrence-in-south-asia•

[DISEC] TOPIC AREA B

The Weaponization of Social Media

Introduction

As one of the most prominent and powerful platforms, social media has been made a medium for the spreading of information to many. Following the use of the Internet for communication purposes by non-state actors such as Hezbollah, the wide spread of radicalized materials has become more rampant in recent years and has served to highlight the great threat that the cyber world poses to the world today. Different motivations, overlapping intentions and methods of various actors can complicate responses.

Terrorist groups such as Daesh and Al Qaeda rely heavily on cyber-based technologies to support organizational objectives. With its ability to publicize, social media allows them to disseminate their information quickly, efficiently, and internationally without having to physically cross borders. With that, the quick spread of data through social media rises and transcends international borders.

For that to happen, online networks provide the perfect platform for mass influence over an audience. The online network's anonymity, transparency and lack of proper surveillance are some of the few characteristics that allow it to be exploited by terrorist groups. The governments' inability to manage data that are posted facilitates the use of social media by terrorists as governments are bounded by the restrictions of laws that were already established. Such surveillance threatens individual rights – including privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society" as stated by the OHCHR, allows terrorists to take advantage of the situation. This brings about a lot of convenience to terrorists and subsequently, the use of social media gives a wide impact to individuals making it one of the most productive and quickest ways to extend terrorists' objectives and messages. Many terrorists ride on the availability of social media to recruit, radicalize and raise funds, and there are many groups who are adroit specialists of this methodology

Social media has become an integral part of the conflict environment over the past 15 years and longer. Starting with what has been labelled the first "internet-war", that is, the Kosovo conflict in 1999, developments have steadily progressed ever since. Counter-insurgency campaigns in Afghanistan and Iraq, several conflicts between Israel and its Arab neighbors, particularly with Hamas in the Gaza strip and Hezbollah in Lebanon, and events in connection with the Arab awakening (or spring), especially the during NATOs operations in Libya, the on-going civil war in Syria, and most recently during the crisis in Ukraine, the world has seen social network media being used more and more strategically by multiple state and non-state actors to create effects in both the virtual and physical domains. Western liberal democracies, however, still look at war in a classical manner and therefore fail to grasp the new realities of contemporary war and the nature of its goals.

War is no longer about states against states (in the conventional sense), but about identity and identity claims, and about cosmopolitanism (inclusion) versus particularism (exclusion / nationalism). Contemporary wars are therefore more about control of the population and the political decision-making process than about control over territory. Contemporary wars are therefore not to be understood as an empirical category but rather as a logical framework in which to make sense of contemporary conflicts and their characteristics. Furthermore, as most conflicts and wars for western liberal democracies today are what is called "wars of choice", requiring a high degree of legitimacy, and multiple non-state actors are struggling to mobilize support and find new ways of fighting asymmetrically, social network media seems to have become the weapon of choice.

The increasing strategic uses of social network media, and the effects achievable in and through the use of them, empower a multitude of actors and have a re-distributive effect on international power relations. This also affects the character of contemporary conflicts. This development is clearly demonstrated in several contemporary conflicts such as in Libya, Syria, counter-insurgency operations in Iraq and Afghanistan and, lately, the conflict in Ukraine. They indicate that social network media and the cyber domain have framed past strategies and actions, and are likely to do so in future conflicts as well. There is also a visible trend of social network media being used for creating strategic effect in contemporary conflicts, which therefore to a higher and higher degree is to be seen as an "instrument of power", not least by non-state actors but by states as well. It is therefore as a result necessary to appreciate the potential game-changing properties of social network media in today's global information environment in all policy, strategy formulation and operational planning. There is, however, a much broader aspect to consider as well.

Social network media technologies are pervasive and have an impact on every aspect of our lives. Issues such as security, privacy, terrorism and activism, and even everyday social

interaction are now all influenced by social network media. At the same time new concerns about privacy arise due to new forms of activism and terrorism, e.g. cyber-activism and cyber-terrorism, emerge, and the responses to the becomes more pervasive. This also creates new concepts for using social network media. This tendency is also seen in contemporary conflicts where web-pages, internet based web-television, social network sites (e.g., Facebook and Twitter), blogs and upload services (e.g., LiveLeak and YouTube) are being used as sophisticated weapon systems. This is the case not only in the "contest of narratives" and perceptions but also when it comes to actual weapon systems or platforms designed to collect intelligence, single out targets, facilitate command and control, and other actors' access to it, not least when disseminating propaganda and conducting deception.

The emergence of new war-fighting concepts, and the evolution of existing ones, has necessitated a discussion of the terminology and policies of social network media and how this technology is brought to bear in conflicts. From cyber-activism to cyber-terrorism, different perceptions of this issue are easily observed. There seems to be a growing acceptance that, along with the social network media technologies, the lines between terrorism, cyber-terrorism, activism, so-called "hybrid warfare" and full-scale conflict have become blurred. The actors and their activities can co-exist in the same conflict domain, and alter agendas and affiliation very quickly, from day to day, as the conflict unfolds. While an act is regarded as terrorism by some, the same act may be considered as activism in the eyes of opposing groups, while in a third instance, it is viewed as operational support for a state actor. This is also the case in respect to social network media.

Definition of Key Terms

Internet: A Global Network of interconnected computers and other devices linked together through certain standard protocols. It provides services such as the World Wide Web, the Cloud, Email and Social Media. Resolution A/HRC/32/L.20 now states access to the internet as basic human right.

Social Media: A tool utilizing internet connected devices to create and share different forms of media in virtual hubs or communities such as but not limited to Text, Pictures, Videos, Etc. This allows for greater reach of content and ideas.

Censorship: The act of removal or hiding of data from public matter to suppress the spread of information which may be of harm to the Censoring authority or its associates. In regards to the internet, censorship is the controlling or suppression of data or media which can be viewed, shared or accessed on the internet.

Privacy: A right guaranteed by the United Nations, it is the right of an individual or group to hide information about oneself and to express oneself in a selective fashion. In regards to the Internet, Resolution 68/167 (The right to privacy in the digital age) of the UN GA defines and adapts the right to privacy for the digital era.

Cyber Warfare: The Act done by a State or Non-State on another by means of the internet or other forms, in order to disrupt the computer networks and infrastructure of the target is referred broadly as a cyber-attack. These are attacks ranging from corporate espionage to database leaks.

Extremists: An individual, but usually a group who hold extreme beliefs on his or her ideals and wishes that they be spread to others by ways seen as inhumane but the majority.

Internet Governance Forum: A forum under the United Nations which acts as a body of discussion on how the internet should be governed. The body was established in the year 2006 under the Secretary-General

Key Issues

Cyber Warfare: With advancements in data storage and use of the internet, it has become a battleground for countries and non-state groups to fight one another often leading to damage to civilian lives. Two such attack has targets such as mass infrastructure, as seen in the Stuxnet attack on Iranian nuclear centrifuges, resulting in over 900 of them being damaged beyond repair with no trace of the origins of the attack and a United States of America plot in 1982 which used faulty computer programs to cause one the world's largest non-nuclear explosion in the Trans-Siberian gas pipeline. Along with these, breeches of private data held by companies can be leaked and has led to personal data of employees and customers being leaked, as seen in the United States Office of Personnel Management (OPM) data breach targeting the records of as many as four million people. It thus becomes imperative that when dealing with warfare as a whole, Cyber warfare and its effects cannot be ignored. Many countries have established task forces, such as India and The United States of America. The United Nations Maintains the International Multilateral Partnership Against Cyber Threats (IMPACT) which acts as a platform for both private and public entities to strengthen the world's readiness to such forms of warfare.

Social Media as a Tool for Terrorists: The advent of social media and its effects has led to a new generation of ideas being propagated through it. Unlike traditional media, Social media is an open media with little control over content published on them and responsibility on the creator

themselves. In recent times the uses of social media have taken a dark turn.

Various Uses: Social media has been used by terrorists and extremist to widen the outreach and support of their ideas, the right of free speech should not apply to these cases as the content sited can do harm to the general public (this is debatable). Terrorists have also been known to use the internet as a form of communication to plan and execute real world attacks, showing us that virtual effects have real world implications.

A tool for recruitment and funding: Terror organization require both massive funding and a large number of real world fighters and now they are employing social media to forms groups of people who sympathize with them, eventually these people possess a high risk of joining the terror groups. This method has shown its effectiveness in western countries, on social media such as Facebook and primarily twitter.

Retaliation from the sites: This activity has not gone unnoticed by the companies who run the sites and they have taken steps, such as shutting down twitter accounts supporting these acts and flagging YouTube videos suspected for terrorism. The effects of these acts have not been very significant as newer accounts are created and videos are often uploaded.

Privacy and other Social Implications: Even with the introduction of the resolution specified in the key terms, privacy online is a very grey area with disparities across borders. The lack of data protection and Strong censorship as seen in the People's Republic of China shows that the idea of a free and neutral internet is always at risk. It becomes imperative that a stronger, global and well-rounded policy be made on privacy on the internet.

Crimes targeting civilians: The digital era has brought with it new threats of crimes against civilians and bystanders, allowing global connections has led to truly global crimes, identity thefts and credit fraud from halfway across the world have caused real life damages. To track down and shut down these organizations and individuals requires global cooperation and agreements which we lack at the moment. Such crimes are hard to track, and even harder to prevent, and with websites regularly putting their users at risk the issue at hand is one of truly global proportions.

How Social Media is used for Military Activities:

Targeting

Targeting is an activity or process that can be described as the guidance concerning the coordination of target nominations (targets and target audiences) in support of the creation of subversion, sabotage and espionage. It is therefore a process to coordinate and synchronize the desired effects with the other activities, conducted in or through social network media, which should create the effects in time and space. Increasingly, targeting is now not just about the selection of conventional military targets but also includes a recognition that effects can be achieved in other ways – some of those may be through social network media – and thus targeting is increasingly being regarded as a full-spectrum activity with hard kinetic power at one end (in this regard, e.g., Hacking or defacing a social network media account) and softer effects at the other (such as deception). The use of social network media for intelligence therefore affords actors with more options in regard to monitoring, tracking and targeting of potential persons, groups, nodes or networks, platforms and content (e.g., existing narratives and actual messaging) of interest. Intelligence collected can thus be used to nominate targets – be that social media profiles, sites, accounts, computers behind these (system level), where to place information (words and images) and other content, influence conversations, how to link things and / or directly address target audiences in order to influence their perception. Finally, intelligence collected from social network media can be used for identifying and nominating targets in the physical domain based on geo-tacked pictures and updates and more. Conversely, information from social network media conversations can also be used for “Bomb Damage Assessment” (BDA) in order to verify the effect of traditional employment of weapon systems (e.g., air delivered munitions, artillery etc.).

Prominence in social network media makes people, as well as their platforms and accounts, targets in contemporary conflicts. Finding and affecting or influencing an opponent’s presence in social network media is therefore an integral part of cyber-warfare, and hence of contemporary conflicts. As seen in Libya, Google Maps and cell phones were used to map regime positions, which were then passed on to NATO, which used the information to nominate targets and engage these with air power. To use this approach, however, requires intelligence preparation, as the information retrieved from social network media needs to be verified by other intelligence sources before they can be used for targeting for air operations. US Central Command (CENTCOM) in Tampa, Florida, is very aware of this constraint. Urgent Twitter messages with targeting information have multiple times been sent from Syria, calling for CENTCOM to initiate bombing missions against Islamic State units and installations outside, e.g., the Kurdish town of Kobane. Using @Centcom, #Kobane and #USHearKobane, Kurdish fighters have tried to get CENTCOM’s attention and provide targeting information and data. At a much more

practical level, also as seen in, e.g., Syria, information from social network media has been used by various actors to target individuals posting information on their accounts and to single out accounts and profiles for computer network attacks or hacking. The latter is possibly also the case regarding the group "Cyber Caliphate's" hacking of CENTCOM's Twitter and YouTube accounts in January 2015, supposedly on behalf of the Islamic State.

Intelligence

Intelligence can be seen as the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning countries or areas of interest, to include specific domains that are not geographical in nature, such as the global information environment. But Intelligence collection is also an activity in itself. In respect to social network media, intelligence is about monitoring online activity and behavior in order to collect and aggregate information and data on and from networks, sites and platforms considered as social network media, including the persons and personas behind them. This is all in order to analyses this information and data to generate knowledge and understanding in general and in particular in order to support the targeting process. Some of what differentiates intelligence collection in social network media from other intelligence activities is the possibility for overt or covert crowdsourcing and the mapping of narratives. Intelligence analysis of social network media can include but is not limited to Trend, Network, and Sentiment, Geo, Content, Behavioral, Systemic and Information analysis. All of these analysis forms can, in turn, contribute to more specific target audience analysis (TAA) and content development in support of psychological warfare or selection of targets for "cyberoperations" in and through social network media. Social network media analysis is therefore a strategic tool for uncovering insights into the posted content, trends, networks and online behavior of audiences and other stakeholders.

In the context of systemic intelligence collection and analysis, it offers a detailed picture of networks, actors, and related communication (interaction), with the help of monitoring tools, all of which has to be tailored to gain a comprehensive understanding of the social network media information environment. It also provides possibilities for mapping who the disseminators, influencers or key opinion-makers are and how they drive the conversation around topics of interest, and people's conversations and actions online that can be mined for insights and understanding. What also makes social media particularly interesting within an intelligence context is the possibility for collection of real-time data – depending on the speed of monitoring and analysis software.

In addition to this, social network media allows for intelligence collection and analysis without boots on the ground, or even physical presence in the area of interest (theatre of operations), this feature of social network media (analysis) makes it particularly interesting from a "remote warfare" point of view, which is when access to an operational area is initially contested or even impossible for several reasons (political mandate, Rules of Engagement (RoE) or for security reasons), or when mostly non-state actors desire to create effects within a conflict area. Libya and Syria are good examples of this. Basically it provides options for leveraging online sharing and conversations in "theatre of operations", which ultimately can lead to engagement with, or targeting of, current and future audiences and influencers.

Cyber-Operations

Cyber-Operations can generally be divided into three separate but complementary activities; Computer Network Attack (CAN), Computer Network Exploitation (CNE) and Computer Network Defence (CND). The first two can furthermore be categorized as "offensive" and the third as "defensive". The offensive operations referees in this contest primarily to activities associated with "computer network attack" (CNA. This can include Distributed Denial of Service (DDoS) attacks on websites (example Blog), the breaching (hacking) of pass-word protected chat sites, e-mails or cell-phones, with the purpose of later exposing the content; intrusion on news agencies' cable news and altering news stories; or altering content and imagery on, e.g., a Facebook profile, etc.; or pinching identity information like usernames and passwords. It can also be intrusion into, e.g., databases in order to, undetected, extract information for intelligence purposes.

Attempting to manage or shape perceptions through trying to control what is available online and what is not can serve as an example of "operations" directed at social network media. The Russian-Georgian war in 2008 started on 7 August, but computer network attacks on social network media started already on 27 July, or 10 days before the conventional military confrontation between Russian and Georgian forces started. Although not verifiably attributed to Russia or an agent of the state of Russia, it has often been claimed that Russia was behind the attacks. The shaping activities consisted of DDOS attacks, defacing and distribution of malicious software. The desired effects seemed to be aimed at creating confusion and hampering the Georgian governments command and control and especially its ability to disseminate crisis management information to the Georgian public. Operations directed at social network media have also created even more tangible offline effects.

Psychological Warfare

One of the potentially fertile areas for weaponizing social network media is the psychological warfare (PsyWar) area. Psychological Warfare refers in this context to those activities associated with influencing a target audience's values and belief system, their perceptions, emotions, motives, reasoning, and, ideally, their behavior. Self-evidently, this involves inducing perceptions, attitudes and behaviors favorable to the originator's objectives. This might be done either overtly or covertly. Covert operations under one are sometimes referred to as "black operations" or "false flag tactics", and could involve untruthful attribution of information or the source behind specific information (content) or outlets (social network media platforms). This is counter to NATO doctrine but has been well demonstrated by Russia's recent incursions into Ukraine and the Crimea. Target audiences for such operations could be governments, organizations, groups, and indeed even individuals. Such was the case in 2008 when Georgia's President Saakashvili was directly and personally targeted. PsyWar can also include activities such as Deception, Propaganda and Subversion.

Utilizing cross-media communication methods PsyWar conducted in and through social network media can be very effective, particularly when used in combination with more traditional means of communication and media, as seen with Islamic State. However, this description of PsyWar can be problematic since it suggests a high level of the use of clandestine methods and activities normally associated with "propaganda", a term which has a distinctly, and unfair, negative connotation. In most western military doctrine, there is normally a distinction between activities that seek to "inform" the media - "Public Affairs" (PA) or Media Operations - and those more concerned with "Influencing" the media as part of a process of reaching opposing or hostile audiences – which in military terminology is more commonly known as, psychological operations (or PsyOps). There therefore exists a debate over "Inform" versus "Influence" functions, at least in western liberal democracies, as it is contrary to the most basic values of not lying to the press and the public. This self-same debate is emerging over the use – by militaries –of social network media – is this use to influence or just to inform? – And to what extent should our own soldiers be allowed to use social network media? The latter issue is also tied to operational security (OPSEC) concerns, and considerations over the sustainment of social network media competences within own forces by a potential ban on the use. Regardless of the political, legal and ethical debates within western liberal democracies and their militaries over the use of social network media, non-state (and some state) actors use social network media very actively for propaganda purposes and do not delineate between the concepts of Inform and Influence. They use social network media exclusively for Influence purposes.

Firstly, looking at how social network media are used to "expose" opponents' wrongdoings or to embarrass them. Non-Governmental Organizations (NGOs) and Human Rights movements, but also groupings that wish to de-legitimize a regime, have for example used "Geo-Bombing" to expose a regime's wrongdoings. This means that they have added imagery of human rights violations and testimony on YouTube and linked them with Google Earth and Google Maps. It is also seen that information stemming from hacking mobile phones, Facebook accounts, Skype conversations and e-mails have been leaked to the media, or onto other social network media sites, in the hope they will go viral and then either undermine an opponent's credibility or legitimacy, or create a hype (in the media) where perceptions not realities matter when the agenda and news discourses are being set. The latter is illustrated by the Russian-Ukrainian crisis where phone conversation between the Estonian Foreign Minister and the EU's Head of External Action Service (EU's Foreign Service) Lady Ashton was recorded and released – allegedly by Russia – in order to undermine the credibility of the EU as an actor in the crisis (first released on Vkontakte, and then picked up by a Russian television station). A counter-move was made by some Estonians, who allegedly accessed a mobile phone conversation between Russian diplomats in Africa congratulating each other on the success in Crimea. All of these exposures were released on social network media. Whether or not the content is correct, however, is not always that important when it comes to PsyWar utilization of social network media. Merely influencing the media discourse, and thereby ensuring that a specific story dominates the airwaves for a while, can be an objective in itself in order to divert media attention away from other current issues.

Regime counterattacks on the rebels, or rather the effect of them in the "Twitterverse" and their effect on public opinion through mainstream media (primarily Al-Jazeera) was a turning point in the conflict in Libya in 2011. Would this effect have occurred without social network media – most likely yes - but it would have required mainstream news media's presence in the country, which the regime tried to avoid. As a result, what was tweeted played a large role in informing international news discourses. Similarly, grainy cell phone imagery of Gaddafi's body, videotaped and uploaded in real-time and reaching YouTube within minutes and shortly after international media (Al-Jazeera) had an enormous influence on the decision-making of the remaining parts of the Libyan regime and further resistance collapsed within hours. Influencing through social network media is probably one of the central issues when it

comes to "weaponization" and the techniques to do so are constantly being developed.

Defence

Defensive operations refer to the protection of own social network media platforms, sites, profiles and accounts in the form of "computer network defence" (CND) at the technical or system level. Information assurance (IA) – a term that denotes the continuous efforts to ensure the integrity of information posed – and at the human level Operational Security (OPSEC) and Counter Intelligence (CI) are both terms designed to prevent the loss of sensitive information and counter external threats. Defensive activities can include the use of, e.g., encryption, anti-tracking and IP-concealing software in connection with social network media.

Defence, as discussed above, a part of unconventional warfare, or the "military" use of social network media in general, can also be to use or provide encryption and circumvention systems, tools and software in order to avoid detection, monitoring and tracking and thereby avoid potential physical repercussions. Lack of appreciation of "operational security" (OPSEC), and lack of awareness about basic cyber-security have cost many rebels, in particularly in Syria, their lives. In contemporary conflicts, nearly everybody has access to and uses social network media for many different purposes. This includes troop contributing nations to international missions, their soldiers and families and news media as well as the warring factions, local populations and third parties to include non-state actors and activists. This use of social network media results in that OPSEC and other defensive issues are of growing concern. Amongst these concerns is, of course, hostile intelligence collection and online deception (e.g., fake profiles, false content attribution and pinching of identity information).

Command and Control

Social network media can be used for Command and Control (C2) purposes. In respect to social network media, C2 is about internal communication, information sharing, coordination and synchronization of actions and facilitates more agile decision-making. Command and Control generally applies to endeavors undertaken by collections of individuals and organizations of vastly different characteristics and sizes for many different purposes. The most interesting and challenging endeavors are those that involve a collection of military and civilian sovereign entities with overlapping interests that can best be met by sharing information and collaboration that cuts across the boundaries of the individual entities.

This is often the case when looking at, e.g., non-state actors, who like opposition groups in Syria, have a need for distributing information, internally and externally, and for coordinating and synchronizing actions, and in some cases giving commands or direction and guidance (D&G) to other groups or entities. Particularly when these groups or entities have no formal structure or are dispersed over large geographical areas, social network media can afford them with means and capabilities to conduct C2 activities. They have, though, to be very cognizant of operational security (OPSEC) issues. Command and Control is scalable. At an organizational level, C2 is about shaping the organization and determining its purpose and priorities. Information and output from this process can, of course, be distributed through social network media to the rest of the organization. The more interesting elements are, however, at the "mission" level. At the mission level, C2 is about employing the organization's assets and capabilities (people, systems, material and the relationships between them) towards a specific objective or task.

Social network media have for long been used by terror-organizations for communicating and coordinating efforts and thereby for command and control purposes. It has, however, emerged in a much more systematic form in Syria, where remote command and control nodes played a large, practical coordination and logistical role. An example of this utilization of social network media is the Mumbai terrorists that had a "control room" in Karachi where social network media, among other media, such as mobile devices, was used to coordinate the actions of the terrorists, partly based on feed-back gained through the monitoring of mainstream news coverage of the terror-attack, and partly based on conversations about the event in social network media. Similarly, in the conflict in Libya, Twitter was used to coordinate information, medical requirements, radio frequencies and telephone numbers along with new satellite frequencies for TV stations that were being jammed. These are all examples of social network media being used for command and control purposes.

Irrespective of the character of an organization – national armed forces, rebel / insurgent group, political activists or some other form of non-state actors, the principles of effects-based thinking (changing the context in which a situation is understood), can be applied to all their activities. All actors, state or non-state, can benefit from collecting intelligence or basic information, selecting targets and achieving effects on these targets, be it physical, informational or cognitive; and furthermore, protecting or defending themselves against other actors' similar activities and utilizing the possibilities for communicating, coordinating and synchronizing their activities in the manner that social network media affords. Even though this monograph has divided them into six distinct activity areas

(intelligence, targeting, psychological warfare, operations, Defence and command and control), they are all mutual supportive, and at least two, often more, will be conducted simultaneously to create the desired effects (often in concert with activities in the physical world). In any case, the maximum effect is achieved through a high level of planning and coordination. The desired effects, associated with each of the activities, can be achieved either on social network media itself (the platforms or networks) or through social network media on humans in order to affect perceptions, attitudes and ultimately behavior. The one half of the desired effects therefore targets the system level (technology). This half is therefore implicitly linked to "cyber-operations" and, e.g., "computer network attack" but can very well also have cognitive effects. The other half of the desired effects therefore targets the informational and social levels of the information environment. The achievement of effects at the systemic level can also be the precondition for the achievement of effects on the informational and or social level(s). One thing, however, is the theory behind an effects-based approach to using social network media as a weapons platform in contemporary conflicts; another is how it has been done so far empirically.

Case Study: The Social Media Battle Space of Syria

"The Syrian conflict is the world's first cyber civil war. Cyber communications are central to strategy and tactics employed by both Assad and the rebels". This statement was put forward by Rafal Rohozinski, who is leading the Canadian based firm SecDev Group's efforts on monitoring internet activities in Syria. He goes on pointing out "that it is hard to overstate how heavily both sides depend on cyber tools to articulate their narrative, stories, themes and messages. The war has integrated kinetic and information warfare tactics in an unprecedented way". The internet and, especially, social network media are used for Command and Control (C2) purposes, providing lines of communication between dispersed groups for coordination and synchronization of tactics on the ground. It is also used for intelligence purposes, including surveillance and reconnaissance, obtaining and maintaining Situational Awareness (SA) through, e.g., "crowdsourcing" of information from denied areas and to receive training and advice on military matters from actors outside Syria. Last, but definitely not least, the cyber domain and social network media are used by all actors to wage Psychological Warfare in order to influence and shape perceptions, attitudes and behaviors of audiences, both inside Syria and internationally. The Syrian civil war is thereby the first to occur in the full throes of the modern information environment saturated by cyber, where mobile technology, social network media and tech-savvy digital natives have created a potent mix influencing the character of the conflict.

The use of the cyber domain for warfare is not new, though. The first signs of this tendency were seen for real already back in 1999 under the NATO-led Kosovo Air Campaign (Operation Allied Force) over Serbia and Montenegro, where the use of e-mails began to be a widespread way of communicating information about what was happening on the ground during the air campaign. The BBC reported back then: "There is a problem with the personal accounts of the war – how do we know they are true? It is easy to spot the propaganda Web-sites [sic] of the actors such as NATO or the Serbia Ministry of Information, but e-mails are supposedly individual points of view rather than concerted campaigns attributable to the actors. Yet they could be written en masse by government press officers or by hoaxers in California". Operation Allied Force is often claimed to have been the first "internet war", where the use of the internet, and whatever cyber tools existed then, for the first time played a noticeable role and had an ability to influence aspects of how the war was fought. The tendency has since been increasingly visible as the technology has developed and afforded multiple actors with an even larger online toolbox or capability for waging war in the cyber-domain.

Christopher Burnett wrote in 2000: "We are engaged in a social netwar." The information age of the late 20th Century has enabled activists to work together globally while maintaining local autonomy. The power of this movement arises from its structure; namely a decentralized network capable of instant communication, collaboration, coordination and action. The implications of this movement are profound and amount to what has been called an 'associational revolution' among non-state actors that may prove as significant as the rise of the nation state". With the war starting in Iraq in March 2003, and later on in Afghanistan, the use of social network media started to play an ever-increasing role. Terror organizations and insurgent groups began using social network media to undermine the legitimacy and credibility of the US led Multinational Force (MNF), targeting the will of troop contributing nation's populations and political decision-makers to discontinue their presence in Iraq. The objective for the insurgent groups was to shift the center of gravity (CoG) away from the physical battlefield and into the cognitive domain – through words and images on social network media. A consequence of this was that terror organizations and insurgent groups now had direct access to their intended audiences. This minimized their reliance on mainstream news media, who had acted as gatekeepers, to get their message out and achieve one of their strategic objectives; undermine their opponent's political will, while at the same time building support for their cause.

Another consequence was that the audiences were no longer restricted Iraq internally, but became global. Already from an

early point in time in Iraq, this showed itself to be a major challenge for western military forces, which had not yet fully learned to fight in the social network media domain of the information environment. As Dr Niel Verrall from UK Defence Science and Technology Laboratories (DSTL) also points out when he questions "whether military commanders fully understand and appreciates the range of activities where social media could provide added value and demonstrate operational impact". By 2005, Al-Qaida had fully realized this. Illustrated by an alleged correspondence between the then number two in Al-Qaida, Ayman AL Zawahiri, and the leader of Al-Qaida in Iraq, Abu Musab al-Zarqawi, intercepted by US intelligence: "I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a battle in a race for the hearts and minds of our Umma" [Muslim community].

Firstly, it shows that Al-Qaida as an organization is well aware of the importance of media to their fight. Secondly, that the fight is as much internal as it is external, when it comes to affecting perceptions and behaviors. Terror organizations now use social network media extensively for all elements of their 'operations'. This was exemplified by the Westgate Mall attack in Nairobi, Kenya, in September 2013, when the Somali Al-Qaida affiliated terror-group Al-Shabaab live-tweeted the attack from at least two different Twitter-accounts, and of course the Islamic State's use of social network media as previously discussed. Other conflicts in the Middle East between Israel and Hezbollah in Lebanon (2006) and between Israel and Hamas in Gaza (2009 and again in 2014), respectively, also show how social network media was used to varying degrees of success by all parties. Initially the Israeli Defence Forces (IDF) was not particularly adept at using social network media, giving Hezbollah an advantage arguably so large that it enabled Hezbollah to portray itself as the both victim and victor of the conflict in 2006. Lessons identified from the 2006 Lebanon war allegedly drove the IDF development of an "offensive" capability within social network media. This capability development continued up to the 2009 Operation Cast Lead in Gaza against Hamas rule, effectively changing the way the IDF conducted its information operations to include the use of social network media. Little attention, however, has been devoted to Hezbollah's exploitation of information as a kind of 'war-fighting function' with social network media as the weapon of choice.

The IDF has continuously developed their social network media capability ever since. The 2006 Lebanon war between Hezbollah and Israel showed early on how social network media was successfully used in a contemporary conflict by a non-state actor to mitigate a conventional military disadvantage. Hezbollah was militarily outclassed by the IDF in all areas, yet they managed to exploit tactical engagements between the IDF and Hezbollah fighters on the ground through an information-led strategy creating strategic effects through primarily social network media. Hezbollah essentially out-maneuvered the IDF land campaign in the information environment and thereby denied Israel the achievement of its strategic objectives. Effectively shifting the Centre of Gravity (CoG) from the physical battle to the information environment, Hezbollah succeeded in creating and sustaining regional and international pressure that eventually forced Israel to cease its operations before achieving its stated strategic objectives. Hezbollah heavily leveraged social network media to influence the political will of key global strategic audiences, including the Israeli population. Hezbollah "packaged" (recorded / filmed, narrated and disseminated) tactical events to include both own successes and Israeli mistakes and major kinetic destruction of sites in Lebanon in a well-coordinated multi-channel cyber-strategy. The desired effect(s) was to demoralize the Israelis, mobilize internal, regional and international support and, in turn, erode support for Israeli policy, recruit new members and at the same time undermine IDF credibility.

At the same time, Hezbollah also managed to exploit Israeli soldiers' unauthorized use of cell phones during the operation by turning hacked and intercepted information from cell phones into propaganda products, effectively exposing compromising cell phone conversations and images. Hezbollah also used social network media for command and control and to defend their main information distribution channel (Al-Manar TV) from IDF cyber-attacks. Information (propaganda products) was, besides being aired over AlManar TV, re-distributed regionally and globally through PowerPoint presentations, video-clips and photos with an attached story in e-mails, video up-load sites, social media and blogs. Through the cyber-information strategy, Hezbollah effectively was able to claim a strategic victory despite the absence of a clear military victory. In the 2009 Hamas-Israel conflict, the hostilities on the ground were mirrored by cyber-informational and social battles for hearts and minds in the social network media sphere. Both sides extensively used, among other social platforms, blogs, Wikipedia, YouTube, Twitter and Facebook to tell their different versions of the events and to a high degree coordinated the online social network media activities with traditional media and diplomatic activities.

The IDF furthermore, besides setting up a new organization to handle this aspect of the conflict, developed their traditional Psychological Operations (PSYOPS) activities even further. PSYOPS were not just a question of radio broadcasts and leaflet drops but also included SMS text messaging to Hezbollah combatants and Lebanese non-combatants, which meant taking PSYOPS into the social network media sphere.

Both Hamas and the Israelis also mobilized "patriotic hackers" and online activists to engage in a cyber-battle for control over the social network media sphere. This was done through "force multiplication" activities, such as creating supportive online communities and networks as well as through direct computer network attacks on, or hacking of, the opposition's social network media accounts and platforms. While this electronic battle in the social network media sphere went on, the traditional media was to a large extent denied access to the battlefield, effectively leaving social network media as the primary source of information for many. Israel also succeeded in shaping the news coverage itself through turning the sheer use of social network media for warfighting purposes into a "process story" in mainstream media. Through the mainstream news' coverage Israel also got their content out indirectly. In turn, this attracted even more attention to their online presence and their social network media accounts and platforms. This tactic has to a great extent been mirrored by the Islamic State in their 2014 social network media efforts.

It is, however, not only in "inter-state"-like conflicts such as Israel-Hezbollah (2006) and Israel-Gaza (2009) that the use of social network media in conflicts has developed. During the so-called "Twitter Revolution" in Iran, in 2009-2010, in connection with election protests and riots over the presidential election, social network media also played a noticeable role as a tool for political mobilization and distribution of documentation on regime's abuses to the outside world. This directly affected the policies of the international community and individual nations such as the United States. The US government allegedly asked the company behind Twitter to delay a software update in order to facilitate the continued use of the platform by the Iranian demonstrators. The Twitter Revolution was the first instance, which received major international attention, of social network media being used for large scale political mobilization, but certainly not the last.

Starting in late 2010, a wave of anti-authoritarian uprisings and rebellions, originating in Tunisia, and then spreading to Egypt, Libya, Bahrain, Yemen and Syria and destabilizing several other Middle-Eastern regimes, transformed the political landscape of the Middle East. "The Arab Spring" or the "Arab awakening" is also often associated with the widespread use of social network media. It is, however, much debated if social network media started the "uprising" or mainstream television started it – in media terms. Social network media, nonetheless, for certain helped spread and sustain it, and quickly became the tool of choice for organizing and coordinating events throughout the Middle East. As well as distributing information and documentation about the events. The uprisings themselves were based on more deeply rooted causes. However interesting, what started the Arab awakening is not the focus here, but rather how the social network media, due to their digital connectivity, was used to mobilize the predominantly urbanized youth in these countries.

Throughout the uprisings the use of social network media continuously developed in response to the dynamics of the situation, including the quick circumvention of any attempts to limit communication, by the quick exploitation of new technological developments. For example, the introduction of new technology as "speak-to-twitter" based on analogue landlines, when regimes (as the Egyptian one) had cut off access to the internet and mobile connections in order to avoid further mobilization of the "masses". It took only two days for Google engineers to build a system, based on international telephone numbers that people could call and leave a voice message that would be transformed into a Twitter feed. This enabled protesters in Egypt to send tweets even though the internet was shut down. It also allowed for outsiders to listen to the tweets on www. This case also shows that for-profit companies are active participants in the contemporary conflict information environment. A tendency that has evolved since to a point where employees of these companies today are targets for, e.g., terror organizations like the Islamic State in Syria and Iraq due to the active role they play in combatting the distribution of terror propaganda on platforms like Twitter, for instance.

The Arab awakening also shows that "Virtual platforms provide not only free speech. They can also mobilize a large mass of people. You have to know that you're not the only one on the court who demonstrates against the System". This observation illustrates the ability of social network media to create perceptions of "critical mass" that again create a sense of security and provide "social proof" for individuals to join a movement or participate in an event. Initially, whether real or unreal is not an important distinction, the perception of the critical mass's existence informs behavior in real life. These mechanisms, brought about by the agile and strategic use of social network media and the constant development of technology and software to support it, are in a very real way able to create changes! Changes in who is empowered and in the distribution of power itself within the international system in contemporary crisis and conflicts.

As a part of the Arab awakening, the situation in Libya went from protests in mid-January 2011 to a civil-war-like situation in February 2011. The world saw here how the Libyan rebels used the internet to mobilize protesters, and to gather internal, regional and international support. The rebels, however, also actively used the internet, and in particularly social network media, for gaining military knowledge from the outside. One, now rather famous, e.g., of this is involves three persons from

different parts of the world; one in Finland, one in England and a rebel fighter on ground in Libya. He put out a "request for information" not to his peers but through crowdsourcing. Between the three of them, via a Skype call over mobile phones they found a solution, based on their collective knowledge that enabled the rebel fighter to engage and successfully destroy the rocket launcher in real time. The Libyan conflict also illustrated how international news organizations used social network media, sometimes as the primary source of information for their coverage of the conflict. For example, Al-Jazeera used Twitter-feeds extensively to substantiate their stories about how the conflict in Libya unfolded on the ground.

Furthermore, the conflict in Libya also showed some of the first tendencies for using social network media in a more operational way. NATO allegedly used social network media for intelligence collection, targeting and Bomb Damage Assessment (BDA) as a supplement its more traditional military intelligence capabilities. The use of social network media for operational purposes, though, is filled with challenges, including the severe difficulties associated with attribution and authentication of content. One small case from Syria shows this clearly. In 2010, it caught the attention of the world media when the news about a Syrian lesbian blogger in Damascus spread globally very quickly. Just as quickly, however, the world found out that "she" was a "he", more precisely, a middle-aged American man named Tom MacMaster, based in Scotland. This case illustrates just how difficult the attribution of the information disseminated on social network media really is. The Syrian conflict, however, offers many other examples of how social network media has been used by the regime, rebels and a variety of external third parties. These examples also illustrate how actors continuously develop their capabilities based on experiences from earlier conflicts to weaponize the use of social network media in order to achieve "political" or "military" effects.

Limitations and Risks

All though social network media presents a series of opportunities for creating "military" effects for state as well as non-state actors, there are at the same time certain limitations and risks associated with the operational use of social network media. The use of social network media for intelligence purposes can, for instance, only be a supplement to other intelligence collection activities. Likewise, it is associated with a series of legal challenges. Due to the massive amounts of data exchanged on social network media, it is probably not possible to monitor, track and map all connections, content and behavior within a network. Hence, even though supported by analysis software, intelligence collection through social network media, like other intelligence collection assets, must be focused on specific topics (prioritized intelligence requirements), and targeted on areas or individuals / profile-accounts. Due to the sheer volume of traffic online, the actor collecting information through social network media will also likely be limited by resources.

The overall utility of information gathered through social network media is also affected by the speed of which things develop online versus the speed with which the information can be analyzed, verified and utilized in operational planning or for, e.g., targeting. Another limitation in this context is the analysis of the peculiarities of social media content like abbreviations, slang and idiosyncratic dialects that are commonly used. Besides the organizational and technological limitations and risks that are associated with the use of social network media for operational purposes, some things stand out in particular. Importantly, online behavior and content can be false and subject to deception and manipulation in multiple ways. Many actors, especially in conflict areas, desire to be anonymous or impersonate as someone else, e.g., to spread propaganda and misinformation or for the purpose of deception. This can, however, also be attributed to operational security reasons for personal protection.

The content can also simply contain wrong information, either on purpose or because the content has mutated and is now misrepresenting the original content through being used in user-generated content in different ways. Furthermore there is a risk that parts of one's intelligence collection plan (ICP) can be compromised and what you are looking for (intelligence requirements) and why (intentions and plans) can be revealed to opponents or third parties. This is particularly the case with crowd sourcing. Security protocols and operational security must therefore be applied, even though the collection of information from social network media is predominantly open source intelligence (OSINT). Also due to the risk of being subject to online deception, manipulation of information (written content, pictures, and video) and impersonation (source attribution) the verification of information gathered is imperative. On the other hand, some of this verification can come from analyzing large quantities of image data from the same area. If hundreds of pictures and video from a particular place or incident exist, it is harder to manipulate. Also the use of software to reveal to which extent a picture has been used elsewhere and is now used in a wrong context can assist in this. There are many examples of pictures from other conflicts being used in current conflicts out of context. E.g., Hamas using pictures from Lebanon claiming they are from Gaza, pictures from Iraq being used as proof of war crimes in Syria and pictures from Kosovo are being used by Pro-Russian rebels in Ukraine claiming Ukrainian war crimes. The common

denominator is that the pictures are taken from internet sources and used in social network media user generated content. Regardless of the limitations and risks associated with the use of social network media for operational purposes, however, it is simply a fact that these media and the technology that facilitates them are a part of the contemporary conflict environment. In other words, they have been weaponized!

Scope of Debate

Discussion of the issue requires delegates to come up with specific and effective solutions to solve the issue so as to diminish the impacts of the spread of radical ideologies. Furthermore, debate should address factors that contribute to the usage of social media as a tool for terrorism.

First would be to tackle the issues of social media – discussing its flaws, the sources of these flaws and thwarting these flaws. Delegates should come together to discuss exactly how these factors had allowed social media to be exploited. Flaws of social media include its anonymous behavior, transparency and lack of proper surveillance. Its anonymous behavior and transparency are one of the few characteristics of social media which made it so popular and widely used by people all around the world. However, due to improper use of social media for radicalization, it has come to a point that social media's positive nature has been overturned. Finding the roots of the flaws of social media would make it easier to thwart the underlying loophole that serves as an opportunity for these terrorists.

Delegates should also discuss how terrorist groups make use of social media and why is social media so favorable and effective. This is the main question that delegates would be circling around. Delegates should further question themselves what the role of social media is in this situation, who are involved, where are the recruits mainly from, why are a certain group of people targeted, and last but not least how is it that these terrorists have the upper hand and exactly what is the role of the governments in the situation.

Major Parties Involved and Their Views

People's Republic of China: The People's Republic of China has been in the forefront when it comes to policies which aim to censor and stifle the free flow of data on the Internet. The Golden Shield Project, often called The Great Firewall of China, is a mass censorship and surveillance system that is operated by the Government. Its main aim is to Block content which criticizes the state and its policies through various advanced methods. The country has also gone on the offensive, launching attacks and creating the Great Canon of China, which serves to shut down and cripple foreign sites.

United States of America: The United States of America, or more specifically the NSA (National Security Agency), has been involved with the Mass Collection of data from both domestic and international sources. It has breached the privacy of Millions of people and infringes on foreign sovereignty by means of the internet. The data collected is used for counter terrorism but this is debatable as it could also be used for the gains of the United States. The organization functions with little oversights and has been the attention of the media after recent events. The USA is also victim to the most cyber-attacks as many sites store their data in servers in the USA.

Russian Federation: Many accusations have been placed on the Russian Federation for participation in Cyber Warfare by employing groups to hack enemy Cyber Infrastructure. This is evident when NATO (North Atlantic Treaty Organization) computer were hacked by a State sponsored group. Russia has also been accused of creation of malware that caused a blackout on the Ukrainian Power Grid. Along with China, they are one of the largest origins of cyber-attacks. These Accusations have been refuted by Russia. Russia during the cold war was victim to a cyber-attack shutting down its Trans-Siberian gas pipeline by means of a virus in the program used to operate it.

Non-State Actors (Terrorists): In the recent years, to boost their area of influence, terror organizations such as but not limited to, Al-Qaeda and Daesh (ISIL/ISIS). Al-Qaeda used the internet as a means to send messages of the group to the masses and as a secure line of communication using self-made software known as 'Mujahedeen Secrets'. Many videos of the leader of the group were posted on the internet, circumventing the need to distribute them to news channels. Through the internet they were able to distribute unedited versions of the same and face lesser censorship. Meanwhile Daesh has grown its online presence exponentially, especially on social media. The group has been known to Upload Propaganda images and videos, and in the recent times, they have uploaded the beheadings of their hostages. Along with this they maintain Al-Hayat Media Center; it acts as the propaganda and media outlet of the group and publishes a magazine called Dabiq in a large number of western languages. As mentioned above they have used these sites as tools and spreading propaganda with very little checks. As such many countries and sites have taken proactive steps to remove their presence from the Internet.

Social Media Sites: Being at the forefront of the spread of propaganda by Terrorists and having access to such large user bases, Companies such as Facebook, Twitter and YouTube have large power on the media consumed by the people and what information can appear on their sites. As such they have become targets not only by terror organizations to exploit but hacker groups also wish to gain access to the vast data stored on the company servers potentially using it against the users of the sites. Co-operation with these companies must be achieved if policies are to be properly implemented.

United Nations: The UN has recognized the need for comprehensive policies on privacy on the internet but has done little for the misuse of social media and overall cyber warfare. Along with this currently existing resolutions are not enforced on the member states thus they are not showing their intended outcomes. As an Intergovernmental body, The UN must take a hand as resolving this global issue.

Proposed Solutions

One approach could be by having Governmental regulation. Governments may look into the data that are posted and to carefully establish measures such as placing blocks on certain types of posts and to remove recruitment websites. They can also choose to remove data through servers; however the downfall to this solution is that it is restricted to the governments' on countries due to international laws.

A simple yet effective approach would be combating terrorism with education. It is important to raise awareness as anyone could be a victim of terrorism and it is important to ensure that we stay away from being swayed by their methods. Education promotes tolerance and respect for diversity and differences which would certainly go a long way. It is also one of the easiest ways to reach youths, who are UNAS Model United Nations Preparatory Conference The Sixth Edition Page 6 of 7 one of the most targeted groups of people terrorists often attack. Through education, spreading information and safety precautions to masses would help facilitate strengthening the resilience of the people against these ideologies.

Lastly would be putting in place a metric for identifying possible accounts associated with terror groups. This includes finding words, terms and hashtags that could be used linked to the recruitment or even misuse of social media. As terrorist groups tend to change their methods and adapt accordingly, trends and natures of terrorist groups also play a part in identifying the accounts. These accounts would be terminated so as to avoid further spread of radicalized information.

Questions a Resolution Must Answer

1. Has social media been weaponized?
2. How has social media been weaponized?
3. How has this affected the character of contemporary conflicts?
4. What techniques and tactics do non-state actors employ to support their political and military aims using social media? What effects can they achieve?
5. Do your solutions cover both the long term as well as short term aspects of the issue?
6. How does this issue affect censorship and the right to freedom of speech?
7. Who are the targets of weaponization and why are they vulnerable to being such targets?

Bibliography

UNHRC. "Promotion And Protection Of All Human Rights, Civil, Political, Economic, Social And Cultural Rights, Including The Right To Development : Written Statement / Submitted By Maarij Foundation For Peace And Development" Accessed on November 14, 2016. https://documents-ddsny.un.org/doc/UNDOC/GEN/G14/114/17/PDF/G1411417.pdf?OpenElement

Audiense "[Interview] How The UN Uses Twitter To Bring The World Together One Tweet At A Time' Accessed on November 14, 2016. https://audiense.com/interview-case-studyhow-the-un-united-nations-uses-twittersocial-media-to-bring-the-world-togetherone-tweet-at-at-time/

Forbes "ISIS is dramatically expanding its presence on Twitter" Accessed on November 14, 2016. http://www.forbes.com/sites/niallmccarthy /2015/03/09/isis-is-dramaticallyexpanding-its-presence-on-twitterinfographic/#5d096e412676

The Hill "FCC says it can't shut down ISIS websites" Accessed on November 14, 2016. http://thehill.com/policy/technology/26043 8-fcc-says-it-cant-shutdown-onlineterrorist-activity

United Nations OHCHR "The right to privacy in the digital age" Accessed on November 14, 2016. http://www.ohchr.org/EN/Issues/DigitalAg e/Pages/DigitalAgeIndex.aspx

Telegraph " how terrorists are using social media" Accessed on November 14, 2016. http://www.telegraph.co.uk/news/worldne ws/islamic-state/11207681/How-terroristsare-using-social-media.html

Sitepronews " How social media is used for terrorism" Accessed on November 14, 2016. *http://www.sitepronews.com/2014/09/22/s ocial-media-used-terrorism/*

Centre for Complex Operations "CHAPTER 13 Recruitment and Radicalization: The Role of Social Media and New Technology" Accessed on November 14, 2016. *http://cco.ndu.edu/News/Article/780274/c hapter-13-recruitment-and-radicalizationthe-role-of-social-media-and-new-tech/*

The Guardian "My granddaughter loses sleep over terrorism': children's fears over global events" Accessed on November 14, 2016. https://www.theguardian.com/society/2016 /nov/01/my-granddaughter-loses-sleepover-terrorism-how-children-respondglobal-events-brexit-childline

The Atlantic "War goes viral" access November 2016 *http://www.theatlantic.com/magazine/arch ive/2016/11/war-goes-viral/501125/*

European Parliament "Religious fundamentalism and radicalisation" Accessed on November 14, 2016. http://www.europarl.europa.eu/EPRS/EPR S-briefing-551342-Religiousfundamentalism-and-radicalisationFINAL.pdf

FBI "Terrorism" Accessed on November 14, 2016. *https://www.fbi.gov/investigate/terrorism*

Academia "Daesh and Social Media platforms" Accessed on November 14, 2016. http://www.academia.edu/14333143/Daes h_and_Social_Media_Platforms