DISEC STUDY GUIDE 2015

CAMUN 2015

A short summary of all there is to know for this year's GA1

Dear Delegates,

Welcome to CAMUN 2015! I am Sarah Alani and I will be your chair for the First Committee, DISEC. This study guide is just the beginning to your exploration on the topics we will be coming across; make sure to do research over the three topics and on your own country's position. Ideally, extensive reading should be done beyond this study guide to ensure readiness into the discussion of these topics, as well as the development of your solutions.

I look forward to seeing you in January!

Table of Contents

Introduction to DISEC

The Disarmament and International Security Committee (DISEC), also known as the First Committee, is one of the six main committees of the General Assembly of the United Nations. After the World War II, a lot of weapons that were conventional were being used for destruction on a mass scale. The committee initiated as two different committees namely the Atomic Energy Commission and the Commission for Conventional Armaments. DISEC – Disarmament and International Security Committee was founded when the United Nations was created. It is the United Nation's first general assembly. All the United Nation's member states form the committee for DISEC. Each of the member states has ***one vote***. A simple vote is passed in the majority to pass the resolutions. It takes up disarmament and international security matters in the light of the general principles of cooperation in 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 the issues of *nuclear non-proliferation, illicit traffic of small arms, and regional militarization*.

The United Nations established the DISEC committee with the purpose of serving as a forum for all representatives of member countries of the United Nations so that they are able to debate on various issues related to security and disarmament in an environment where equality prevails.

Relevant measures are taken by the committee to reduce or prevent conflicts and hostilities between various countries on matters that the Security Council of the United Nations does not discuss. Fostering security, disarmament and peace all over the globe, is the main purpose and role of DISEC.

DISEC has focused on some of the issues relating to nuclear proliferation, trading of small arm, the Arctic Circle security and cyber-security, since the past few years. Some of the other recent crisis handled by DISEC is disputes of territories and resources underwater. Natural resources over the world are depleting and ice caps are melting. Accordingly many of the nations have begun venturing deep into the ocean and further away from coasts in the effort to obtain raw materials. Also showing up are tensions in many areas including South China Sea which increases the need for a proper framework to use, discover and develop resources under the water. Accordingly the morality and legality of establishing military bases on the offshore have been considered by DISEC. Economic, social and political problems are created at the established foreign military bases. A framework is created by DISEC for closing, operating and establishing of foreign military bases. This year's DISEC at CAMUN will call upon the threats of cyber-warfare, investigate the perils biological weapons and discuss the sensitive issue of the Arctic region. A committee is only as good as its delegates and we hope that our delegates tackle these issues in a constructive and practical manner.

We hope the DISEC committee will be a stimulating and engaging one for all in concern.

Topic 1: Resolving the threats of cyber-warfare and addressing cyber security

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" Bruce Schneier

Introduction:

Cyber-warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. RAND (a corporation) research provides recommendations to military and civilian decision makers on methods of defending against the damaging effects of cyber-warfare on a nation's digital infrastructure.

Network outages, data compromised by hackers, computer viruses and other incidents affect our lives in ways that range from inconvenient to life-threatening. As the number of mobile users, digital applications and data networks increase, so do the opportunities for exploitation.

Cyber security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Its importance; Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

During a Senate (House Armed Services Committee) hearing in March 2013, the nation's top intelligence officials warned that cyber-attacks and digital spying are the top threat to national security, eclipsing terrorism. In red are the nation states considered to have offensive capabilities; the others have only defensive capabilities. Defensive cyberspace capabilities direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; to outmaneuver adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable freedom of action in cyberspace. This line of operation can trigger offensive cyberspace operations or other response actions necessary to defend networks in response to hostile acts, or demonstrated hostile intent.

	Cyber warfare		CW training/ Trained Units	CW exercises/ simulations	Collaboration w/ IT Industry and/or Technical Universities
	Doctrine	Strategy			
Albania		X	X	X	
Argentina	X		X		
Australia		X	X		
Austria	X		X	X	
Belarus	X		X		
Brazil		X	X	X	
Bulgaria		X		X	
Canada				X	
China	X		X	X	X
Cyprus		X	X	X	X
Czech Republic		X	X	X	
Denmark		X		X	
Estonia		X	X	X	
Finland	X			X	
France	X		X	X	X
Germany	X		X	X	
Ghana		X			
Hungary		X	X	X	X
India	X		X	X	X
Iran			X		X
Israel	X		X	X	X
Italy			X	X	X
Japan			X		
Jordan		X	X		
Kenya			X		
Latvia		X	X	X	
Lithuania		X		X	
Malaysia		X	X		
Netherlands		X	X	X	
New Zealand		X	X		
North Korea			X		X
Norway		X		X	
Pakistan			X		
Philippines		X	X		X
Poland		X		X	
Russia	X		X		X
Slovak Republic		X		X	
South Korea		X			
Spain				X	
Sweden				X	
Switzerland		X		X	
Turkey		X	X	X	
United Kingdom		X	X	X	
USA		X	X	X	

The targets of cyber-attacks:

From the government agencies to the International Olympic Committee and news media - nearly anything can or has already fallen prey to cyber-attacks. Even well protected security infrastructure such as the Pentagon seems to be vulnerable as has been revealed by a massive cyber-attack in 2008 and in 2011 when approximately 24,000 files were abstracted. Apart from high profile breaches against industrial, financial and governmental targets, it is small companies, which have increasingly become the victims of targeted cyber-attacks due to the fact that their security measures can often be considered rudimentary compared to those of large enterprises. The main goal of attacks against the private sector is to gain intellectual property (industrial espionage), whereas attacks against government agencies aim for strategic

intelligence, sensitive security data or in general the disruption or destruction of private and public networks. Alternatively, cyber-attacks in the form of hacking, have also become a new way of protest and "civil disobedience". An EU study conducted by the European Network and Information Security Agency analyzed more than 140 reports from the security industry and other organizations. It concluded that the top threats could be categorized in 6 areas: mobile computing, social technology, critical infrastructure, trust infrastructure (defined as "any information system that provides strong authentication and aims at establishing a trusted, secure connection between two end points."), cloud computing and big data. Furthermore, it pointed out that particularly the threats to trust infrastructure and mobile computing are on the rise. Typical targets of cyber-attacks include electrical grids, telecommunication systems, web servers, enterprise information systems, media corporations and newspapers (lately for instance France 24 and the NYT), banks, corporations in the technology sector but also in the construction sector or even agriculture, satellite systems, pipelines, air traffic control systems, water systems, ministries and other organizations affiliated with governments as well as non-governmental organizations.

Prominent cyber-attacks:

The "Original" Logic Bomb: in 1982 a computer control system stolen from a Canadian company by Soviet spies caused a Soviet gas pipeline to explode. The code for the control system had been previously modified by the CIA, which had been tipped off, to include a logic bomb, i.e. a piece of code that changes the workings of a system, which changed the pump speeds to cause the explosion. An air force secretary describe d it as "the most monumental non-nuclear explosion and fire ever seen from space"

Titan Rain: the name given by the FBI to a series of coordinated attacks on American computer systems since 2003ongoing for at least three years. It was discovered that several sensitive private and public computer networks were infiltrated by the hackers, such as those at Lockheed Martin and NASA. Not only was military intel and classified data stolen, but also thousands of "zombified" machines, i.e. computers infiltrated by malicious software that can be activated later, were left behind. Titan Rain is considered the largest state-sponsored cyber attacks in history, said to have been organized or supported by the Chinese government.

Korean cyber war: Already in 2009 and 2011 North Korea has been blamed for cyber raids against South Korean organizations. On 15 March, North Korea's KCNA news agency accused the US and its allies of large-scale hacking attacks on its internet servers. Later in March around 32,000 South Korean computers at banks and broadcasters were affected by a cyber attack. Even though the attack could be traced back to a Chinese IP address officials emphasized that this did not reveal who was behind the attack, as hackers can route their attacks through addresses in other countries to obscure their identities. North Korea is suspected to have staged the attack amid rising tensions on the Korean peninsula.

International agreements:

International law regarding real warfare developed within a 150 years. This raises the question whether these regulations could be used in matters of online-warfare. A genuine legal framework, *a jus ad bellum and jus in bello* (Right to war and International humanitarian Law), is still missing for cyber-warfare. The Working Group on Internet Governance, established by the United Nations based on a recommendation from the World Summit on the Information Society, was initiated to agree upon the future Internet Governance. Technical, policy, economic, institutional, as well as legal perspectives were taken into consideration. Two different approaches dominated the debates at the summit. Whereas one side argued for the development of genuine cyber-law since speed and volume of Internet cross-border communication hinders the enforcement of existing legal rules, the other side argued that the Internet is in fact not conceptually different from previous telecommunication technologies. Consequently, existing legal rules could be applied to the Internet and as far as global regulation is concerned, the most efficient option would be the harmonization of national laws, resulting in the establishment of one set of equivalent rules at the global level. The Working Group has fulfilled its duty to give recommendations for the next World Summit on the Information Society. But unfortunately a consensus regarding concrete measures could not be found. For the time being, bilateral agreements are the most common solution for cyber security regulations, like the new security pact of the UK with India. A group of international lawyers, working in conjunction with the International Committee of the Red Cross and the US Cyber Command, has now published a book on the subject. The group of experts was invited to draw up the handbook by NATO's Co-operative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, where the centre was established in 2008 following a wave of cyber-attacks on the Baltic state from inside Russia. The experts explained that existing laws broadly apply to cyberspace. The Tallinn manual contains 95 "black letter rules". However, it is no official NATO document or policy but an advisory manual. Among other things it stipulates that cyber-attacks led by governments must avoid sensitive civilian targets such as hospitals, dams, dykes and nuclear power stations. The manual also states that hackers who participate in online attacks during a war can be legitimate targets even though they are civilians.

Types of attacks:

<u>Vandalism:</u>

Definition: Web vandalism is characterized by website defacement and/or denial-of-service attacks.

Details:

Website defacement is the most common form of web vandalism, so both terms are used interchangeably.

Website defacement is a major threat to many internet-enabled businesses. It negatively affects the public image of the company. Companies may suffer from loss of customers.

How does website defacement work?

- Find a username (e.g., by posing as administrator and calling an employee; administrator information can be retrieved from a database)
- Retrieve the password for that username (e.g., brute-force)
- Obtain administrative privileges
- Begin defacing the website (and install a backdoor)
- How to defend against website defacement?
- Avoid using the server as a client (e.g., web browser)
- Remove buffer overflow vulnerabilities in your programs
- Use a different user(s) other than root for managing the website contents
- Enable access logs
- Update!

Propaganda:

Definition

Propaganda is deliberate collection of messages intended to influence the opinions and actions of large numbers of people. The information provided in these messages is not done so impartially or necessarily truthfully, as the basic purpose of propaganda is to influence the audience towards the side of the propagandist.

Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist. – Garth S. Jowett and Victoria O'Donnell, Propaganda And Persuasion

Importance

Propaganda is a powerful recruiting tool. The web provides a way in which propaganda can be quickly and cheaply disseminated. The cost of publishing propaganda may simply be a web-hosting fee. Through the use of the web's video and file-sharing sites along with social networking sites, propaganda can reach large audiences in a very short manner of time.

Terrorism

Terrorist group Al-Qaeda uses their media arm, As-Sahab (media production house for Al-Qaeda), to spread the group's propaganda. As-Sahab releases audio and video messages through the web, and is doing so at a growing rate (one video every six days in 2006, one video every three days in 2007). The production quality of the videos have also increased, with current videos having sets that would not appear out of place on American news shows like "60 Minutes".

Terrorist groups are also recruiting computer-savvy jihadists to produce sophisticated web videos and other multimedia products. In one case, a militant group in Iraq advertised a website design competition where the prize was the chance to fire three remote-controlled missiles at an American army base in Iraq. Similarly, the Global Islamic Media Front has posted on radical Islamic websites advertisements asking for job applications for a variety of posts for a jihadist-perspective weekly video bulletin.

Denial of service:

Definition

A **denial of service attack** is an attempt to consume all of an available resource in order to keep that resource from its intended users.

More Information

The denial of service attack is one of the most common attacks on the Internet. Its use is so widespread because it is relatively easy to implement and it is very difficult to defend against. Generally, an attacker creates a flood of bogus requests to a service, ignoring the results. The server is bogged down by the large number of incoming requests, taking long times to handle both the fraudulent requests and any legitimate requests that come in during the attack. In extreme cases, the server will not be able to handle the strain of the incoming connections and will crash, permanently breaking the server until it is manually restarted. A denial of service attack may also consist of a request which is crafted to exploit a specific vulnerability in the server, causing it to crash without requiring a large number of requests.

There are many kinds of denial of service attacks. We will go over some of them below:

A **smurf attack** is a denial of service attack based on creating a large flow of traffic to the targeted machine. The attacker sends a "ping" packet to a broadcast address on the network; this broadcast address is a special IP address which specifies all of the computers in a given network. Additionally, the ping packet is forged to have its source IP address set to be the source IP of the targeted computer. Each of the computers which receives the ping packet sends a "pong" packet to the targeted computer; thus an attacker is able to multiply the amount of network traffic he can create to a target by the number of machines on a network vulnerable to this technique.

Ping flooding is sending a large number of ping packets to a target computer. Other than consuming the victim's bandwidth, unless the target computer is configured properly it will also respond to each ping packet with a pong packet, wasting CPU time as well as network bandwidth.

A **SYN (synchronized) flood** is an attack based on sending forged TCP/IP (transmission control protocol/internet protocol) connection requests to the target computer. The target computer opens a connection and responds with a handshake SYN/ACK (synchronized acknowledgment) packet, awaiting an ACK packet from the remote attacker. Because the original request was forged, however, the SYN/ACK is received by no one in particular and thus the request will remain open

on the victim's computer until it times out. This used to be a very useful attack: in 1996, for example, the most common TCP implementation had an "awaiting response" queue only eight entries long, and a timeout of three minutes. An attacker could completely remove a server's ability to respond to legitimate clients by sending eight packets every three minutes!

A **distributed denial of service attack** is a denial of service attack which uses many computers in order to consume the target computer's bandwidth. This is a class of attacks rather than a single attack technique; smurf attacks, above, are an example of a distributed denial of service attacks. Ping flooding and SYN flooding can also be implemented as distributed denial of service attacks. Most denial of service attacks today are distributed, for the simple reason that modern defenses make it easy to block all traffic coming from a single source. Distributed attacks are also advantageous for resource-consumption attacks; the more computers you have consuming resources, the easier it is to consume all of the resource.

Defenses

Defending against denial of service attacks is notoriously difficult. While a single-source attack can be blocked simply by ignoring the attacking computer, a distributed attack cannot be blocked so easily: with many computer requesting resources, it is difficult to detect (and ignore) each attacking computer. In pathological cases, the number of attacking computers may be increasing faster than these computers can be blocked, even with an automated detection solution!

Defending against distributed denial of service attacks is largely a matter of proper router configuration on a level beyond that of the victim's control; even if you can ignore every fraudulent request, it still takes some computing power to determine the validity of each request, and many distributed attacks are on such a scale that even that little loss of computing power is enough to completely shut down the target's computer. However, higher-level routing solutions are possible. Smurf attacks, for example, can be defended against if computers configure themselves not to respond to ping packets sent to broadcast addresses; alternatively, the routers can be configured to not pass along ping packets which are sent to broadcast addresses. SYN flooding has become much less useful in recent years as more and more modern implementations remove arbitrary limits on the number of open connections.

Solving a denial of service attack often requires the cooperation of the administrators of individual systems and administrators of ISPs or internet backbones. The defenders must react to each new attack, determining the proper way to configure their routers so that valid packets are allowed through while fraudulent requests are automatically blocked.

Network Based Attacks against Infrastructure

As in conventional warfare, critical infrastructure serves as a target to cyber-attacks. Although often regarded as the most severe type of cyber-attack that includes power, water, fuel, communications, and transportation, few critical infrastructure attacks have been perpetrated to

this day. Previously, it was thought that the worst a network based attack could do was denial of service. As recently as this year however, hackers were able to inflict physical damage on machinery.

Power, Water, Fuel

Electrical power, water, and fuel supplies are at the core of a country's infrastructure. The disruption of any of these services would have a chain reaction effect and cause severe repercussions. Many of these critical infrastructure pieces are owned and operated by private companies in the United States. For efficiency and cost saving purposes, the control systems of power plants, water pump stations, and fuel lines have been networked and can be controlled remotely. This opens the possibility of an attacker gaining access and taking control.

Economist Scott Borg, who produces security-related data for the federal government, projects that if a third of the country lost power for three months, the economic price tag would be $700 billion.

"It's equivalent to 40 to 50 large hurricanes striking all at once," Borg said. "It's greater economic damage than any modern economy ever suffered. … It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II."

Communications

Nearly all telephone calls are routed at some point through an IP network. This fact, along with the increasing use of pure VOIP calling subjects telephone communications to the same attacks that have plagued data networks since their inception.

Transportation

- Traffic Control

In major metropolitan areas such as Los Angeles, traffic lights are monitored and controlled from a central location.

"ATSAC is a computer-based traffic signal control system that monitors traffic conditions and system performance, selects appropriate signal timing (control) strategies, and performs equipment diagnostics and alert functions. Sensors in the street detect the passage of vehicles, vehicle speed, and the level of congestion. This information is received on a second-by-second (real-time) basis and is analyzed on a minute-by-minute basis at the ATSAC Operations Center"

With central control and networking comes the chance that an outsider will gain access. Two engineers were recently arrested for tampering with the traffic system in Los Angeles during a union protest. Four days were needed to restore the signals.

- Air Traffic Control

Another transportation system connected via a network is the air traffic control system employed at hundreds of airports nationwide. As far back as 1997, the first case of an attack on air traffic control systems was reported

"As a result of a series of commands sent from the hacker's personal computer, vital services to the FAA control tower were disabled for six hours in March of 1997."

What has been done?

"I can't say it [the vulnerability] has been eliminated. But I can say a lot of risk has been taken off the table," said Robert Jamison, acting undersecretary of DHS's National Protection and Programs Directorate in response to the vulnerability discovered in power generation equipment. The US-Computer Emergency Readiness Team (US-CERT) has decided to develop an "early warning system" to alert the public about the risk of cyber-attacks. Experts in security have had mixed responses since attacks are hard to see coming in advance. In January 2008, President Bush also signed an order called the "Cyber Initiative" to overhaul US cyber defenses with one particular goal of reducing the number of outside internet gateways from over 4000 to fewer than 100.

Conclusion

The area of cyber-security and warfare is complicated, often falling in a grey area, given the great variety of perpetrators and crimes. Delegates must be able to draw up solutions to not only individual cases, but also international conflicts, keeping national securities as a top priority.

References:

http://www.rand.org/topics/cyber-warfare.html

http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

http://www.natcom.org/commcurrentsarticle.aspx?id=1963

http://www.scalable-networks.com/wp-content/uploads/2011/04/Introducing-a-Cyber-Warfare-Communications-Effect-Model-to-Synthetic-Environments-2010.pdf

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.

Topic 2: Biological warfare

Introduction

Since prehistoric times, humans have used available technologies for destructive and beneficial purposes. Biological weapons have often been pronounced as the 'poor man's nuclear bomb'. *Biological warfare is defined as the 'intentional or threatened use of viruses, bacteria, fungi or toxins from living organisms to produce death or disease in humans, animals or plants.* They can result in destruction of crops, temporarily discomforting a small community, killing large numbers of people, or other outcomes. They have been discussed between governments and in the medical literature, and have been the subject of frequent commentaries. The mention of 'biological warfare' often elicits a sense of deadly mystery, as summarized by a Russian journalist: "I have been gathering information on biological weapons (BW) for several years. Out of all the means of mass destruction, this kind can be considered as the most mysterious."

BW agents can cause large numbers of casualties with *minimal logistical requirements*. Perpetrators can escape long before BW agents cause casualties, due to the incubation periods of the agents. Weapons are easy and cheap to produce and can be used to selectively target humans, animals, or plants. The costs of conventional weapons ($2000), nuclear armaments ($800), and chemical agents ($600) would far outstrip the bargain-basement price of biological weapons ($1) to produce 50% casualties per square kilometre. Biological agents are much deadlier than chemical agents: *An estimated 10 grams of anthrax could kill as many people as a ton of nerve agent Sarin.* Furthermore, molecular biology and genetic engineering have enabled scientists to increase the virulence, develop antibiotic resistant strains and create novel strains of pathogens for which the population lacks immunity.

Agents can be easily procured from the environment, universities, biological supply houses, and clinical specimens. Common fermentation techniques used for producing antibiotics, toxoid vaccines, foods, and beverages can be used to grow large quantities of biological agents. Simple aerosol generating devices mounted on planes or trucks, as used for crop-dusting, can generate 1-5 micron particles ideal for causing infectious aerosols. BW agents are typically invisible in aerosol clouds and may not be detected until humans become ill. Panic would result as medical capabilities are quickly overwhelmed.

Biological weapons, like chemical weapons, radiological weapons, and nuclear weapons, are commonly referred to as *weapons of mass destruction*, although the term is not truly appropriate

in the case of biological armaments. Lethal biological weapons may be capable of causing mass deaths, but they are incapable of mass destruction of infrastructure, buildings, or equipment. Nevertheless, because of the indiscriminate nature of these weapons—as well as the potential for starting widespread pandemics, the difficulty of controlling disease effects, and the simple fear that they inspire—most countries have agreed to ban the entire class.

Multiple factors confound the study of the history of biological weapons, including secrecy surrounding biological weapons programs, difficulties confirming allegations of biological attack, the lack of reliable microbiological and epidemiological data regarding alleged or attempted attacks, and the use of allegations of biological attack for propaganda and hoaxes. However, a review of historical sources and recent events in Iraq, Afghanistan, Great Britain, and the United States demonstrates that interest in biological weapons by state-sponsored programs, terrorist organizations, and criminal elements is likely to continue.

Background information

The direct use of infectious agents and poisons against enemy personnel is an ancient practice in warfare. Indeed, in many conflicts, diseases have been responsible for more deaths than all the employed combat arms combined, even when they have not consciously been used as weapons.

Early attempts:

The early use of biological weapons included the *contamination of water* with animal carcasses and filth. Another ancient tactic was to allow an enemy to *take sanctuary* in an area endemic for an infectious agent in anticipation that the enemy force would become infected, for example, allowing unimpeded access of opposing forces to areas where transmission of malaria was highly likely.

The Carthaginian leader, Hannibal, used early biological weapons (serpent toxins) in the naval battle of the Eurymedon against King Eumenes of Pergamum in 184 BC. Hannibal ordered earthen pots filled with serpents to be hurled onto the decks of the Pergamum ships. The pots shattered on impact, releasing live serpents among the enemy sailors. The Carthaginians exploited the ensuing panic and chaos to win the battle.

One of the most notorious early biological warfare methods was the hurling of corpses over the walls of besieged cities, primarily as a terror tactic. After war broke out between the Genoese and the Mongols in 1343 for control of the lucrative caravan trade route from the Black Sea to the Orient, the Mongols laid siege to Caffa, a Genoese colony in the Crimea. The Mongols were severely afflicted and forced to lift their siege. As a parting shot, they hurled “mountains of dead” over the city wall, in the hope that “the intolerable stench would kill everyone inside.” An outbreak of plague in the city followed. A review of the incident suggests that the introduction of plague into the city by the cadavers—as a result of a successful biological attack—is the most biologically plausible of several competing hypotheses on the source of the outbreak.

Smallpox was particularly devastating to Native Americans. The unintentional yet catastrophic introduction of smallpox to the Aztec empire during the Narvaez expedition of 1520, and its subsequent spread to Peru in advance of Pizarro's invasion of the Inca Empire, played a major role in the conquest of both empires. An outbreak of smallpox at Fort Pitt presented an opportunity to take advantage of the Native Americans' unique susceptibility to this disease. Subsequently (in July 1763), Sir Jeffrey Amherst, British commander of forces in the American colonies, conceptualized a similar plan with Colonel Henry Bouquet, thus sanctioning the concept of use of smallpox as a biological weapon. An epidemic of smallpox occurred among the Native Americans of the Ohio River Valley that year.

The Start of modern Biological Warfare and the World Wars:

The birth of scientific bacteriology during the 19th century provided the scientific and technical basis for modern biological weapons programs. *The Hague Conventions of 1899 and 1904 outlawed the use of "poison or poisoned arms," although the possible use of bacteriological weapons was not specifically identified or addressed.* Germany started the first known scientific, state-sponsored biological weapons program during World War I. The Allies had purchased US draft animals for military use, and German operatives infected these animals with glanders and anthrax while they were awaiting shipment overseas. The Germans also conducted similar operations in Romania, Russia, Norway, and Argentina, with varying levels of success.

The German bio-warfare program of World War I is of special interest for several reasons: it was the *first national offensive program*, the first program to have a *scientific foundation*, and the first confirmed instance of *actual wartime use* of biological agents. It is impossible to determine the effectiveness of this program; although the German operatives involved thought it was a success, no documentary evidence supports this conclusion.

In response to chemical warfare during World War I, the *1925 Geneva Protocol*, an international protocol was formulated. The protocol, developed by the League of Nations' Conference for the Supervision of the International Trade in Arms and Ammunition, addressed warfare methods of nation-states only. *It had no verification mechanism and relied only on voluntary compliance.* This meant that nation states couldn't be kept under check and had no deterrents whatsoever. Many of the original signatory states reserved the right to *retaliatory use*. While prohibiting the use of bio-weapons, the treaty did not seek to prevent the research, production, or possession. There was no provision for inspection. Many countries that ratified the protocol stipulated the right for retaliation. An interesting footnote to history, the United States did not ratify the Geneva Protocol until 1975. Signatories that began basic research programs to develop biological weapons between World War I and II included Belgium, Canada, France, Great Britain, Italy, Netherlands, Poland, and the Soviet Union

Japan: After the defeat of Russia in the 1905 Russo-Japanese War, Japan became the dominant foreign power in Manchuria. In 1932, Major Shiro Ishii, a Japanese army physician with an interest in biological agents, came to conduct human research. Ishii created a secret facility at Beiyinhe, and began experimenting on a dramatic scale. No research study subjects survived; all

died of either experimental infection or live vivisection. These studies continued until a prisoner riot and escape occurred, which resulted in the closing of the facility in 1937. *However, larger and more extensive facilities were subsequently built.*

In 1936 Ishii was made chief of the Army water purification bureau. That autumn the Japanese appropriated 6 square kilometres of land, where Ishii built the massive research facility known as *Unit 731*, where a census of 200 prisoners was kept as expendable subjects of experimentation. Ultimately, more than 3,000 Chinese prisoners were killed after these experiments. Most of the evidence was destroyed at the end of the war, and in all likelihood the actual number *was much greater.*

In 1936 Japan appropriated 20 square kilometers of land near Mokotan, a small village just 6 km south of Changchun, the capital of Japanese-occupied Manchuria. Predominantly a veterinary and agricultural bio-warfare research unit (independent from Ishii's Unit 731), Unit 100 focused on developing biological weapons for sabotage operations. Although animals and crops were the focus of most of the research, numerous human studies were also conducted, similar to those conducted by Unit 731.

Eleven Chinese cities were allegedly attacked during "field trials" using infectious agents including cholera. These attacks may have backfired because up to 10,000 Japanese soldiers reportedly contracted cholera after a biological attack on Changde in 1941. As a result of the Japanese bio-warfare program, 580,000 people are estimated to have died in China. The field trials were terminated in 1943, yet basic research and human experimentation at Unit 731and elsewhere continued until the end of the war.

By the end of the war, the Japanese bio-warfare program claimed to have effective vaccines for anthrax, cholera, dysentery, typhoid, and typhus. Use of biological warfare agents by Japanese forces may have given them an advantage over the Chinese, but results were erratic and prone to backfire. Despite the enormously expensive program (both in terms of national treasure and human lives) and the weaponization of many agents, Japan never developed a *credible bio-warfare capability*, mainly because of the failure to develop an effective delivery system.

Both the United States and the Soviet Union's Biological Warfare program owe their germination to the work of Unit 731. The Soviets captured Unit 731. US forces captured Shiro Ishii and Kitano Misaji and granted them immunity from war crimes if they divulged their BW secrets. US had no research in either offensive or defensive BW early in World War II. Only when the intelligence agents of the Office for Strategic Services (OSS) discovered the activities of Unit 731 did the US initiate its own offensive germ warfare program at Camp Detrick, Maryland in late 1942.

It is interesting to note that the Nazi offensive BW program limited itself to inhuman experiments not unlike Japan's Unit 731. Prisoners in Nazi concentration camps were forcibly infected with a wide variety of bacteria, protozoa and even a virus, Hepatitis A. These horrors were ostensibly experiments done to study pathogenesis and to develop vaccines and sulpha drugs rather than to develop weaponized versions of these pathogens. There is a positive note to

this inhumanity; it was used against the Germans in an area of occupied Poland. Polish physicians in the region used a vaccine (formalin-killed Proteus OX-19) to produce a false-positive test for typhus. German troops were not dispatched to the area to round up its residents for deportation to concentration camps, thus saving an unknown number of people.

The perceived threat of biological warfare before World War II prompted *Great Britain* to stockpile vaccines and antisera, establish an emergency public health laboratory system, and develop offensive biological weapons. "Cattle cakes" consisting of cattle feed contaminated with *B anthracis* spores were designed to be dropped from aircraft into Axis-occupied Europe to cause anthrax among livestock, which would in turn induce famine. In addition, explosive munitions designed to aerosolize and disperse *B anthracis* spores as an antipersonnel weapon were tested on Gruinard Island near the coast of Scotland in 1942. These experiments successfully produced anthrax among targeted sheep. The antipersonnel weapons were not mass produced, and neither the cattle cakes nor the explosive munitions used. *Great Britain continued research and development after the war in conjunction with the United States and Canada and performed secret open-air tests using pathogens in the open ocean near the Bahamas and Scotland till 1955.* Attempts at decontamination by starting brushfires failed as spores of anthrax had been embedded in the island's soil thus making total decontamination impossible to this day. This creates a disadvantage of BW use by a nation; the difficulty in decontamination may preclude the use of acquired territory.

Great Britain's offensive program was ultimately terminated between 1955 and 1956 because of budgetary constraints and *reliance on nuclear deterrence*.

Timeline of events:

June 17, 1925: Geneva Protocol

Spurred by the horrors of World War I, delegates in Switzerland create a Geneva Protocol banning the use of chemical and bacteriological methods of warfare. However, countries are still allowed to research, develop, and produce these weapons. Thirty-nine countries sign the protocol, including the United States. Although the Senate refuses to ratify the treaty, the U.S. government says it will still abide by the terms.

1930

Shiro Ishii is appointed professor of immunology at the Tokyo Army Medical College. He is promoted to the rank of major in Japan's Army Medical Corps and begins to advocate for a Japanese biological weapons program.

1932

The Japanese Army gives Shiro Ishii control of three biological research centers, including one in Manchuria, a Chinese province that the Japanese had invaded a year earlier.

1934: International Biological Weapons Research

Great Britain begins taking steps towards establishing its own biological weapons research project. Although the Medical Research Council is cool to the idea, Fildes agrees to assist the government.

1937

Construction commences on a large Japanese biological weapons complex called Ping Fan near the Manchurian city of Harbin.

Nazi Invasion of Poland, 1939

September 1, 1939

World War II begins in Europe with the invasion of Poland by Nazi Germany.

September 19, 1939

In a speech, German Chancellor Adolf Hitler boasts of fearsome German weapons against which his enemies would be defenseless. This fuels speculations among Allied leaders about what weapons German scientists may be developing.

1940

The Japanese biological weapons complex Ping Fan begins operations. It employs some 3,000 personnel under Ishii's direction, working on a wide variety of biological agents, including bacteria that cause plague and anthrax. Over the next five years, Unit 731, as it becomes known, conducts horrific tests on Chinese prisoners and, allegedly, some Allied POWs. Victims are injected with, forced to eat, and made to breathe deadly pathogens. Often prisoners are killed before the diseases have become terminal so autopsies can be performed. Ishii's men also create bacteriological bombs, and later that year Japanese warplanes repeatedly drop porcelain bombs containing fleas infected with plague over Chinese towns, resulting in several outbreaks of plague among the human population.

November 18, 1941

A committee of nine eminent American biologists convenes at Secretary of War Henry Stimson's request to investigate the possibility of germ warfare.

December 7, 1941: America Joins the War

The Japanese attack Pearl Harbor, bringing America into the war. That same day, British Prime Minister Winston Churchill receives a top-secret memo summarizing developments at Porton Down and reporting that cattle cakes laced with anthrax bacteria are the only biological weapons that currently can be deployed.

January 2, 1942

Churchill's Defense Committee meets and gives the go-ahead for production of these cattle cakes. Later that year, the first of some five million cattle cakes are manufactured at Porton Down. The plan, named, "Operation Vegetarian," is to drop them from aircraft over Germany in the hope of wiping out its cattle. This plan is never implemented.

February 17, 1942

Stimson's committee issues the first of its two reports, concluding that biological warfare is "distinctly feasible" and the United States should begin its own biological weapons program immediately.

April 29, 1942

Stimson writes to President Franklin Roosevelt arguing America must be prepared. In May, Roosevelt approves the creation of a U.S. biological weapons program.

May 27, 1942

British-trained commandoes ambush high-ranking Nazi leader Reinhard Heydrich near Prague. Although he suffers only minor wounds, Heydrich will die suddenly a week later. Fildes later claims to have "had a hand" in the assassination, perhaps by supplying the commandoes with grenades which were contaminated with botulinum toxin.

June-July 1942

The Japanese test Salmonella on Chinese prisoners. Then they disperse the bacteria that cause typhoid, cholera, and other food-borne diseases over Chinese populations.

July 15, 1942: Anthrax Tests Successful

A team of Porton Down scientists led by Fildes begin outdoor testing of anthrax bacteria on the remote Scottish island of Gruinard. They set off anthrax-filled bombs and observe their impact on a group of sheep placed downwind. Most of the sheep die within a few days.

January 19, 1943: U.S. Involvement Grows

Baldwin visits Horn Island, off the Mississippi coast, and will select it as a place to conduct outdoor biological tests.

February 1943

Baldwin locates a site for his work at a little-used National Guard airfield in Frederick, Maryland, that becomes known as Camp Detrick. The Army officially takes it over in March and staff members begin arriving in April. The Army also acquires Horn Island, ret research. Scientists completed interior equipment installation; the boiler was operated by Alex Bryant, then a soldier.

July 1943

Camp Detrick scientists begin outdoor biological bomb testing, using yeast instead of pathogens for the initial trial runs.

March 8, 1944

Convinced that the Germans will use biological weapons if able to produce them and that the British must be able to retaliate in kind, Churchill places an order for 500,000 "anthrax" bombs, i.e., bombs containing anthrax bacterial spores, with the Americans.

August 1945

In Manchuria, Unit 731 is blown up ahead of the advancing Russian Army, destroying most but not all records of Ishii's activities.

September 2, 1945: The Atomic Bomb and the End of WWII

Japan officially surrenders to the United States after atomic bombs are dropped on Hiroshima and Nagasaki, ending World War II.

October 9, 1945

Sanders begins interrogating Tomosada Masuda, a colleague of Ishii's at the Ping Fan facility.

January 3, 1946

The U.S. War Department releases a report on the nation's wartime biological weapons program, keeping many key details obscure.

January 9, 1946: A Deal with Ishii

The U.S. demands that the Japanese government produce Ishii, who is in fact alive; he is handed over to American forces eight days later.

May 8, 1947

Ishii tells Fell that he is willing to share what he knows, including details of his human experiments, in exchange for immunity from prosecution. Hopeful of gathering useful information, the Americans agree. Although Ishii's information is eventually judged to be of little worth, the U.S. honors its immunity deal and no mention is made of biological weapons at the Japanese war crimes trials.

May 8, 1951

North Korea accuses the U.S. of dropping smallpox bombs over Pyongyang; American General Matthew Ridgway calls these accusations “deliberate lies.” Despite the U.S. denial and the independent debunking of several of North Korea’s biological weapons claims, they will be repeated over the course of the Korean War.

March 1952

Chinese foreign minister Chou En-Lai claims that the U.S. is using bacteriological bombs over China. The Chinese form the International Scientific Commission to investigate. Their report concludes that "The peoples of Korea and China have indeed been the objective of bacteriological weapons. These have been employed by units of the U.S.A. armed forces."

November 25, 1969: Nixon Renounces Biological Weapons

Nixon announces that "the United States will renounce the use of any form of deadly biological weapons that either kill or incapacitate," adding, "Mankind already carries in its own hands too many of the seeds of its own destruction." Although Nixon's initial statement does not mention toxins such as botulinum toxin, on February 14, 1970, he will makes clear that those weapons will also be abandoned. As a result of Nixon's Executive Order, the U.S. offensive bioweapons program is terminated; further biological research by the military is limited to defending and immunizing against such weapons.

April 10, 1972

The Biological Weapons Convention, which bans all bioweapons, is completed and opened for signature. Seventy-nine nations immediately sign the treaty

April 2, 1979: International Bioweapons Use

Nearly 70 people die of anthrax in the Soviet city of Sverdlovsk. The government of the U.S.S.R. claims the deaths resulted from people consuming infected meat. The U.S. suspects that anthrax bacterial spores were accidentally released from a Soviet military biological facility (Compound 19), and that the victims contracted inhalation anthrax. If the U.S. view was correct, the Soviet Union was violating the Biological Weapons Convention, which it had ratified in 1975

1980-1988

The Iran-Iraq War features the widespread use of chemical weapons; first by Iraq, then by both sides.

March 16, 1988

As part of a wide-ranging military campaign against the Kurds, the Iraqi government uses chemical weapons against Kurdish cities, such as Birjinni and Halabja. It has been estimated that more than 5,000 Kurds are killed by nerve and mustard agents dropped on them by Iraqi aircraft between March and August of that year.

1989

A Soviet defector from Biopreparat, Vladimir Pasechnik, reveals the existence of a continuing offensive biological weapons program in the U.S.S.R.

April 1991

The U.N. Security Council orders Iraq to stop all biological, chemical, and nuclear weapons programs, and inspectors are authorized to ensure compliance.

April 1992

Russian President Boris Yeltsin admits the 1979 outbreak was caused by the Soviet military, although he gives few details. He also admits that the Soviet Union had operated an offensive biological warfare program in violation of the Biological Weapons Convention. That same year Meselson leads a team of U.S. scientists on a fact-finding mission to the site of the 1979 Sverdlovsk anthrax outbreak.

March 2003

The United States leads an invasion of Iraq. President George W. Bush and Vice President Richard Cheney insist that Saddam Hussein's government possesses weapons of mass destruction, but no such weapons have been found.

Current status of nations:

The chart below details countries possessing or developing CW or BW. It draws on open source intelligence including unclassified government assessments. Taking into account the clandestine and controversial nature of these programs, state capabilities are considered under four headings: State declarations detail the state's official position on the weapons in question and whether they have declared stockpiles or programs. Allegations look at allegations made by other states, namely the U.S. as to what the status of programs and stockpiles are. Potential delivery systems consider the means that suspected possessors have of delivering such weapons. Any other information is also included which may be of relevance to a state's capabilities.

The chart also details whether each state has signed, ratified, or acceded to relevant international treaties: the 1972 BWC, which bans offensive biological weapons development and possession, and the 1925 Geneva Protocol, which forbids the use of chemical and biological weapons in war.

COUNTRY	BIOLOGICAL WEAPONS CAPABILITIES	TREATY STATUS
China	State declaration: China states that it is in compliance with its BWC obligations and that it has never had an active BW program, denouncing such weapons. Allegations: According to the U.S., China's BW activities have been extensive and a 1993 State Department Compliance Report alleged that activities continued after China joined the BWC. The 2010 report indicates that little information is known about China's activities, and that recent dual-use activities may have breached the BWC. Existing infrastructure would allow	Geneva Protocol: Acceded 8/24/29. BWC: Acceded 11/15/84.

	it to develop, produce, and weaponize agents. Potential delivery systems: include cruise missiles, fighters, bombers, helicopters, artillery, rockets, mortars, and sprayers.	
Cuba	State declarations: Cuba denies any BW research efforts. Allegations: A 2003 State Department Compliance Report indicated that Cuba had "at least a limited developmental offensive biological warfare research and development effort." The 2010 report claims that "available information did not indicate Cuba's dual-use activities during the reporting period involved activities prohibited by the BWC." Allegations of BW programs have been made by Cuban defectors in the past. Any other information: Cuba has a relatively advanced biotechnology industrial capabilities.	Geneva Protocol: Acceded 6/24/66. BWC: Signed 4/12/72, ratified 4/21/76.
Egypt	State declarations: Two vague statements alluding to a BW capability were made by President Saddat and one of his ministers in 1972. According to the 2010 report, the Egyptian government remains "committed to the prohibition of the development, production and stockpiling of bacteriological and toxin weapons." Allegations: Various allegations that Egypt had developed BW by 1972 and that it may not have eliminated this capability. The 2010 report records that "available information did not indicate Egypt's biological research and development activities during the reporting period were inconsistent with the BWC." Potential delivery systems: Missiles.	Geneva Protocol: Signed 6/17/25, ratified 12/6/28. BWC: Signed 4/10/72.
India	State declarations: India is abiding by the BWC and will continue to do so. Allegations: Very limited – no conclusive evidence of prior or current offensive programs. The 2010 report records that "available information did not indicate that	Geneva Protocol Signed 6/17/25, ratified 4/ 9/30. BWC: Signed 1/15/73, ratified 7/15/74.

	any of India's biological research and development activities were inconsistent with its BWC obligations." Potential delivery systems: Potential delivery systems include short-range, anti-ship cruise missiles; short-range, air-launched tactical missiles; fighter aircraft; artillery; and rockets. Any other information: Has a strong capability in bio-technological research.	
Iran	State declarations: Has publicly denounced BW. Allegations: The Defense Intelligence Agency alleged in 2009 that Iran's BW efforts "may have evolved beyond agent R&D, and we believe Iran likely has the capability to produce small quantities of BW agents but may only have a limited ability to weaponize them." The 2010 report assesses that there is evidence showing Iran continues dual-use activities, but there is no conclusive evidence showing BWC violations. Potential delivery systems: include short-range cruise missiles; short-range, air-launched tactical missiles; fighter aircraft; artillery shells; and rockets. Any other information: Iran has a relatively sophisticated pharmaceutical industry.	Geneva Protocol: Acceded 11/5/29. BWC: Signed 4/10/72, ratified 8/22/73.
Iraq	State declarations: None by post-2003 governments. Allegations: None since the 2003 invasion of Iraq by a U.S. led coalition. The 2010 report assesses that Iraq is "not engaged in activities prohibited by the BWC." Any other information: Admitted to testing and stockpiling BW in the mid-1990s. These stockpiles appear to have been destroyed prior to the 2003 invasion.	Geneva Protocol: Acceded 9/8/31. BWC: Signed 5/11/72, ratified 6/19/91.
Israel	State declarations: Has revealed little in terms of capabilities or programs. Israel has not given a reason for not signing the BWC. Allegations: There is belief that Israel has had an offensive BW program in the past. There is no	Geneva Protocol: Acceded 2/20/69. BWC: Has not signed.

	conclusive evidence that this is still the case. Any other information: Highly sophisticated pharmaceutical and biotechnical industry.	
Libya	State declarations: Libya announced in 2003 that it would eliminate its BW program and adhere to its BWC commitments. According to the 2010 report, Libya is in full compliance.	Geneva Protocol: Acceded 12/29/71. BWC: Acceded 1/19/82.
North Korea	State declarations: The 2010 report comments that North Korea has yet to declare any of its biological research and development activities as part of the BWC confidence building measures. Allegations: The 2010 report remarks that North Korea may "still consider the use of biological weapons as a military option" Potential delivery systems: include short-range, anti-ship cruise missiles; bombers; rockets; mortars; sprayers; artillery; helicopters; and fighters.	Geneva Protocol: Acceded 1/4/89. BWC: Acceded 3/13/87.
Pakistan	State declarations: None. Allegations: No substantial allegations. The 2010 report states that "available information did not suggest that any agent and toxin research activities by Pakistani entities were inconsistent with Pakistan's BWC obligations." Potential delivery systems: include short-range, anti-ship cruise missiles; short-range, air-launched tactical missiles; fighter aircraft; artillery; and rockets. Any other information: Has ability to support limited biological weapons research and development effort.	Geneva Protocol: Signed 4/15/60. BWC: Signed 4/10/72, ratified 9/25/74.
Russia	State declarations: In 1992, Boris Yeltsin acknowledged that the USSR had pursued an extensive and offensive BW program throughout the 1970s and 1980s. He	Geneva Protocol: Acceded 4/5/28. BWC: Signed

	banned any more of such work being undertaken. However, there is little public information of any more specific declarations of what Russia may continue to possess. Allegations: Agents weaponized included tularemia, typhus, Q fever, smallpox, plague, anthrax, Venezuelan equine encephalitis, glanders, brucellosis, and Marburg. Researched numerous other agents and toxins that can attack humans, plants, and livestock. The 2010 report details that Russia continues to engage in dual-use biological research activities, yet there is no evidence that such work is inconsistent with BWC obligations. It assesses that it remains unclear whether Russia has fulfilled its obligations under Article I of the convention. Potential delivery systems: include fighter aircraft, artillery, rockets, helicopters, short-range ballistic missiles, and cruise missiles. The former Soviet program planned to deliver certain agents, such as smallpox, anthrax, and plague, by ICBM.	4/10/72, ratified 3/26/75.
South Korea	State declarations: None. Allegations: None.	Geneva Protocol: Acceded 1/4/89. BWC: Signed 4/10/72, ratified 6/25/87.
Sudan	State declarations: None. Allegations: No confirmed evidence of a BW program.	Geneva Protocol: Acceded 12/17/80. BWC: Acceded 10/17/03
Syria	State declarations: President Assad has hinted at Syria's procession of a BW capability according to the 2010 report. Allegations: Syria has undertaken activities banned by the BWC. According to the 2010 report, there is no	Geneva Protocol: Acceded 12/17/68. BWC: Signed 4/14/72.

	evidence that Syria has "abandoned its past, stated intentions to develop a biological deterrent." President Obama says the United States is monitoring the situation very closely as civil conflict worsens. Potential that chemical/biological weapons will be used. Potential delivery systems: include fighter aircraft; helicopters; artillery; short-range, anti-ship cruise missiles; short-range, air-launched tactical missiles; and rockets.	
Taiwan	State declarations: None. Allegations: 2010 Compliance Report confirms that "available information did not indicate that any biological research and development activities by Taiwan entities during the reporting period were inconsistent with the BWC." There are "no unresolved BWC compliance issues involving Taiwan." Any other information: Has been upgrading its biotechnology capabilities in recent years.	Geneva Protocol: Has not acceded. Has pledged to adhere to the BWC and CWC.
United States	State declarations: Unilaterally gave up its biological weapons program in 1969. The destruction of all offensive BW agents occurred between 1971 and 1973. Currently conducting research as part of its biodefense program. Allegations: According to a compliance report published by the Russian government in August 2010, the U.S. is undertaking research on Smallpox which is prohibited by the World Health Organization. The U.S. is also accused of undertaking BW research in order to improve defenses against bio-terror attacks which are "especially questionable from the standpoint of Article I of the BTWC." Any other information: In May 2012, the second of the controversial H5N1 avian flu papers was published. The US National Science Advisory Board for Biosecurity advised against publishing due to concerns that the dual-	Geneva Protocol: Signed 6/17/25, ratified 4/10/75. BWC: Signed 4/10/72, ratified 3/26/75.

	use research would be used in bio-warfare.	

UN action:

1925 Geneva Protocol: The 1925 Geneva Protocol prohibits the use of chemical and biological weapons in war. The Protocol was drawn up and signed at a conference which was held in Geneva under the auspices of the League of Nations from 4 May to 17 June 1925, and it entered into force on 8 February 1928. The Protocol recognizes the significance of bringing together controls on chemical and biological weapons. While it prohibits the use of such weapons, it does not prohibit their production, development, and stockpiling, gaps covered by later treaties such as the 1972 Biological and Toxin Weapons Convention (BTWC) and the 1993 Chemical Weapons Convention (CWC). There is no verification mechanism contained within the Geneva Protocol and compliance is voluntary.

The Geneva Protocol, implicitly, does not cover internal or civil conflicts. Moreover, a sizeable fraction of its parties have reserved a right to retaliate in kind if chemical and/or biological weapons should ever be used against them by enemies or allies of enemies. This, and the contractual character of the Protocol, has rendered it a no-first-use agreement.

Biological Weapons Convention: The Biological Weapons Convention (BWC), the first multilateral disarmament treaty banning the development, production and stockpiling of an entire category of weapons of mass destruction, was opened for signature on 10 April 1972. The BWC entered into force on 26 March 1975. The BWC bans:

The development, stockpiling, acquisition, retention, and production of:

- Biological agents and toxins "of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes;"
- Weapons, equipment, and delivery vehicles "designed to use such agents or toxins for hostile purposes or in armed conflict."
- The transfer of or assistance with acquiring the agents, toxins, weapons, equipment, and delivery vehicles described above.

The convention further requires states-parties to destroy or divert to peaceful purposes the "agents, toxins, weapons, equipment, and means of delivery" described above within nine months of the convention's entry into force. The BWC does not ban the use of biological and toxin weapons but reaffirms the 1925 Geneva Protocol, which prohibits such use. It also does not ban biodefense programs.

The treaty regime mandates that states-parties consult with one another and cooperate, bilaterally or multilaterally, to solve compliance concerns. It also allows states-parties to lodge a complaint with the UN Security Council if they believe other member states are violating the convention. The BWC is a treaty of indefinite duration that is open to any country. Notably

absent from the list of member states is Syria, a treaty signatory that the United States believes is probably developing biological weapons.

The convention has been flagrantly violated in the past. The Soviet Union, a state-party and one of the convention's depositary states, maintained an enormous offensive biological weapons program after ratifying the BWC. Russia says that this program has been terminated, but questions remain about what happened to elements of the Soviet program. Iraq violated its commitments as a signatory state with its biological weapons program, which was uncovered by the UN Special Commission on Iraq after the Persian Gulf War. Iraq became a state-party after the war but is thought by the United States to be still violating the convention.

In November 2001, the United States publicly accused Iraq, as well as member state North Korea, of breaching the convention's terms. Washington also expressed concern about compliance by Iran and Libya, which are also states-parties, and by Syria. The United States itself raised concerns in 2001 about whether some of its activities, ostensibly being conducted as part of its biodefense program, are permitted under the BWC. In 2002, Washington added Cuba, also a state-party, to its list of countries conducting activities that violate the convention.

Bioterrorism and bio-crime?

Bioterrorism refers to use of biological agents by a political or religious group or cult (a group not otherwise recognized as an extension of the government of a state) to achieve a political or ideological objective. Bioterrorist incidents have increased markedly since 1985, with two peaks in 1998 and 2001. The 1998 peak followed publicity of the anthrax threat posed by Larry Wayne Harris; the 2001peak followed the September through October anthrax mailings. Successfully executed attacks have been few but high in impact; the 1984 Rajneeshee Salmonella attack resulted in 751cases of infection; the 2001anthrax mailings resulted in 22 cases of infection, five deaths, and approximately 10,000 individuals being offered post exposure prophylaxis. In 1995 in Japan, the Aum Shinrikyo cult released sarin gas in the Tokyo subway system, resulting in 12 deaths and thousands seeking emergency care. Bio-crime refers to the malevolent use of biological agents when the perpetrator’s motivation is personal, as opposed to a broader ideological, political, or religious objective. Although bio-crimes constitute only a small fraction of criminal assaults and are usually unsuccessful, a well-executed attempt may be deadly; the resulting disease may pose clinical and forensic challenges. Bio-crimes have generally been more successful than bioterrorist attacks; 8 of 66 bio-crimes reviewed by Tucker65 produced 29 deaths and 31injuries. What bio-crime and bioterrorism reveal is the dangers of easy accessibility to biological material to the general public. Delegates therefore must also consider the security issues surrounding bio-warfare.

Challenges:

Bio-warfare is an extremely vast and sensitive topic that encompasses several areas including bio-crime (referring to individuals who use these methods for personal reasons), bioterrorism (organizations using it for ideological purposes), medical research, etc. It is also a difficult topic as the lines are blurred on various fronts such as the ascertaining of whether disease was caused

artificially or was a natural outbreak in an area, or whether a nation is conducting medical research, or actually developing bacteria as weaponry. Furthermore, it is cheap to use, is undetectable and allows perpetrators time to leave during the incubation period. Delegates must solve issues including ramification of the BWC, deterrents to using biological weapons, reducing accessibility of these materials, and much more.

References:

History of biological warfare
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBoQFjAA&url=http%3A%2F%2Fwww.ncbi.nlm.nih.gov%2Fpmc%2Farticles%2FPMC1326439%2F&ei=oiS4U7CgBMHJ0AWpqoDICg&usg=AFQjCNFwif8zWrEySQ9azVMY1pZ6q_wWBQ

Biological weapons – a history
https://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CEIQFjAE&url=https%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D19931&ei=oiS4U7CgBMHJ0AWpqoDICg&usg=AFQjCNFwnBn7IDElJW_Ix1uwckG9AVR5EA

Biological Weapons convention
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCUQFjAB&url=http%3A%2F%2Fwww.un.org%2Fdisarmament%2FWMD%2FBio%2F&ei=wiG4U7G0Dsqw0AWfl4GYDQ&usg=AFQjCNHUhyJyUB8ZuvkGnWOWi6rRQVAZnw

Arms control: BWC
https://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0CEcQFjAG&url=https%3A%2F%2Fwww.armscontrol.org%2Ffactsheets%2Fbwc&ei=wiG4U7G0Dsqw0AWfl4GYDQ&usg=AFQjCNE03q5td9lOcsvUK_x5N-aH8_PtrA

1925 Geneva Protocol
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&sqi=2&ved=0CBoQFjAA&url=http%3A%2F%2Fwww.un.org%2Fdisarmament%2FWMD%2FBio%2F1925GenevaProtocol.shtml&ei=0SC4U52dCeTR4QTQqYHwAw&usg=AFQjCNEUzHbn4xxQAYtVooy6MH5I39qG8A

Status of countries with BWs
https://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBoQFjAA&url=https%3A%2F%2Fwww.armscontrol.org%2Ffactsheets%2Fcbwprolif&ei=yR-4U_W7BoyY0AXhqIDwDA&usg=AFQjCNGW6kYwNyITOOf-c9xwCqtPH0Kw6g

A timeline of biological weapons
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CCcQFjAC&url=http%3A%2F%2Fwww.pbs.org%2Fwgbh%2Famericanexperience%2Ffeatures%2Ftimeline%2Fweapon-

timeline%2F&ei=wxm4U4PJBcO70wXumYGACw&usg=AFQjCNGymALsLUtwqsEL_UHoNt0ZspiOXg

From poisoned darts to intentional epidemics
https://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CEIQFjAE&url=https%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D19931&ei=oiS4U7CgBMHJ0AWpqoDICg&usg=AFQjCNFwnBn7IDElJW_Ix1uwckG9AVR5EA

Germ warfare
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&uact=8&ved=0CFcQFjAI&url=http%3A%2F%2Fwww.uic.edu%2Fclasses%2Fosci%2Fosci590%2F7_1Germ%2520Warfare%2520Biological%2520Weapons.htm&ei=XRS4U5y6HqKN0AWEjIHwCA&usg=AFQjCNEcmPBHLRW30KGXr_F9hnecPr2uqQ

Encyclopedia Britannica
http://www.google.ae/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CB8QFjAB&url=http%3A%2F%2Fwww.britannica.com%2FEBchecked%2Ftopic%2F938340%2Fbiological-weapon&ei=9em3U8KJKoWP0AXstICgCw&usg=AFQjCNH6oZOq9bk_y1OnlgRhG52O6ormsQ

Topic 3: Militarization of the Arctic

Introduction

Having long been perceived as a land of mystery yet to be discovered, the Arctic region generally refers to an area around the North Pole that includes the **Arctic Ocean** as well as parts of *United States*, *Canada*, *Russian Federation*, *Norway*, *Denmark*, and *Iceland*. Because it is difficult to determine its borders precisely, the Arctic has, for an extended period of time, been an issue of controversy among numerous nations. Seen in the past as an inhospitable place on Earth, the Arctic is currently attracting world's attention as a jackpot of resources.

Unlike other regions of this world, the Arctic is **not privately owned** by any state in particular; however, despite this fact, many nations, especially those bordering the High North, are currently trying to take advantage of their geographical position by secretly developing military or research centres in different areas of Arctic where they have access. Because the Arctic served as a *transit area* for many nations during World War II, its importance as an uninhibited land that lies in waiting to be utilized were brought into the attention of many states. The boost in its strategic importance led to a previously uninhabited land to become the target victim considered as a potential core of *national security*. Nations are now using militarisation to display their power and claim the Arctic, or at least parts of it, as their own. ***According to the United Nations Convention on the Law of the Sea (UNCLOS), any state has special rights over the exploration and the use of marine resources out to 200 nautical miles from its coast, area known as Exclusive Economic Zone. Thus, there are concerns some would be interested to claim parts of the Arctic as the ice caps shrink.*** Due to an increased human interruption in its recent years, the environment of the Arctic is constantly being damaged—its ice is melting rapidly, endangering most of its rare inhabitants.

The concurrence of three factors sparked the start of militarization of the Arctic: the developments in *military technology*, the *geostrategic factors* specific to its region, and the *East-West conflict*, which intensified the political atmosphere.

Throughout the period of Cold War, the two world powers—Soviet Union and United States—continuously showed great interest and effort in building stable military; the Arctic militarization reached its peak in 1980s, when the many advanced military technologies, such as the submarine-launched ballistic missiles (SLBms), began to play substantial roles in the strategy of the super powers. Correspondingly, such developments led to a greater need for nations

bordering the land for sea and air defence systems, which resulted in their preparation for militarization in case of hostile actions that the two world powers might have had taken.

Russia's plans to start exploring the oil from the region, as "The Arctic belongs to Russia" according to Vladimir Putin, are not only in disagreement with the environmentalists' view but as well with the governments from Canada, the United States and other states neighboring the Arctic. Taking into account the current tensions, it is of utmost importance for the United Nations Security Council to investigate the situation and to determine the existence of a threat to peace. In addition, in order, "to maintain international peace and security", recommending immediate actions represents a priority.

Importance of the Arctic:

The Arctic region is considered to be geographically significant due to several reasons. The primary and utmost reason is that the High North contains an unimaginable abundance of natural resources. A study conducted by the US authorities concluded that the Arctic may be capable of containing an approximate of ***one fifth of the world's undiscovered oil and natural gas resources***; in fact, evidences that suggest the possibility of 90 billion barrels of oil reserves and 47 cubic meters of natural gas lie under the region, which amounts to 13% of the world's estimate reserves. Taking into consideration that the daily consumption of these resources are trivial compared to this number, it could be assumed that these great amount of hidden resources could meet global need for up to 3 years.

In addition to oil and natural gas, the Arctic is also believed to be rich in other resources, including such *precious stones* as platinum, gold, silver, iron, zinc, copper, as well as significant deposits of *methane hydrates*, the potential future energy source, deep under the region's ocean. In a situation where the world's natural resources are being depleted at an extremely fast rate, it is desirable for any nation to claim Arctic as its own land, which presents a profusion of natural resources along with a *vast area of developable land*. Although at the present, technology is not yet advanced enough to extract all the resources believed to be kept in the Arctic, the fast rate of scientific technology's evolution suggests that such knowledge will be available soon.

Furthermore, the major effects of climate change—*global warming*—is most visible in the Arctic. One other factor that contributes to the significance of this region results from this global climate change. As the annual global temperature rises gradually yet constantly, the vast land Arctic land is **decreasing** in size, with sea ice and ground permafrost melting rapidly. As a result, in recent days, it has been possible for some ships to pass through areas that were near inaccessible before the climate change. In 2005, for instance, the *Akademik Fydorov*, a Russian Research vessel, successfully reached the North Pole without the aid of an icebreaker. Another case would be the two German ships traveling from South Korea to Siberia through the Northeast Passage. Looking at the current situation, some scientists predict that the Arctic would be *completely free of ice* in near future. This conclusive prediction leads to an implication that

new shipping routes through the Arctic will become much shorter than the currently existing ones. If such is the case, then both time and finance can be saved in *transportation and trade*.

Glossary

Militarization

The process by which a society prepares for violence, through such means as to equip with armed forces, military supplies, etc.

The Arctic States

Arctic States refers to the five nations that border the Arctic region, which include: Canada, Denmark, Norway, Russian Federation, and United States.

The Ilulissat Declaration

An outcome of the meeting of the five Arctic States, the Ilulissat Declaration presents a common position of these five nations on issues such as sovereign rights, environmental change, and maritime security.

Timeline

September 1996 –Establishment of the Arctic Council under the Ottawa Declaration; its members include: Canada, Denmark, Finland, Iceland, Norway, Russian Federation, and United States

December 2001 –Russian Federation submits claims to the U.N. for an extended continental shelf; the claim is rejected and more evidence demanded

November 2004 –The Arctic Climate Impact Assessment is released by the Arctic Council

March 2007 –Breaking the Ice conference on trans-Arctic shipping is held in Iceland

May 2008 –The five Arctic States (Canada, Russia, United States, Norway, and Denmark/Greenland) sign the *Ilulissat Declaration*; not invited to this meeting were indigenous groups, Finland, Iceland, and Sweden.

January 2009 –NATO seminar on Security Prospects in the High North is held in Iceland

June 2011 –NATO Parliamentary Assembly meets in Tromsø, Norway to discuss what role organizations such as NATO and the EU might play in relation to economic and strategic trends in the High North.

Major Countries/Organization Involved and Their Views on Arctic Militarization

Russian Federation

Russia views the Arctic region as an area of crucial importance to the country's economic and strategic interests. Several times, Russian officials stated the Arctic is in Russian territory. According to Moscow, the eastern Lomonosov Ridge represents an extension of the Siberian continental shelf. Conversely, after an official submission into the UN Commission on the Limits of the Continental Shelf in 2001, the conclusion was that additional research must be done before Russia can lay claim on the Ridge. Thus, in August 2007, the Arktika 2007 expedition continued the exploration in order to bring evidence that will eventually prove the Russian hypothesis. Russia concluded this expedition by leaving a Russian flag in the seabed. Arctic is, on one hand, a vital source of resource, **producing 11%** of the nation's GDP; on the other hand, it provides Russia with access to three oceans and military bases, which grants numerous advantages in terms of geographical position. In consequence, Russia ***strongly opposes the internationalization of the Arctic***; it plans to deploy special military forces in the region in order to "guarantee *military security* under various military and political situations."

United States

Shortly before his resignation, George W. Bush issued a presidential directive dedicated to the United States Arctic Policy, emphasizing the strategic significance of the Arctic for the United States in relation to the *missile defense and early warning systems*. United States also implied that US is also entering the *scientific and military race for sovereignty* over parts of the Arctic. However, US takes a different approach from Russia in that it has always supported the need for ***freedom of navigation*** in the Arctic Ocean, focusing on the fact that its vessels have the right of international navigation both through Northwest Passage and straights along Northern Sea Route. Due to the fact, that the USA has not ratified the UNCLOS, the American government can make no official claims on the Arctic. Nevertheless, considering that the "Prudhoe Bay Oil Field" from Alaska`s North slope is the largest oil field in North America, research in the region represents a priority.

Canada

The prime minister of Canada announced the creation of ***two military bases*** in the Canadian Arctic; to underline the determination of Canada to maintain its sovereignty in the Arctic, he also declared that eight patrol vessels would be built and deployed in this region. Likewise, Canada considers the attempts of US and EU for freedom of navigation in the Arctic as *questions to Canadian jurisdiction* regarding navigation safety in the Northwest Passage. Canada believes that the passage is part of its internal waters and thus *should be regulated by the Canadian national law.*

Denmark

Denmark is engaged in a territorial dispute with Canada over the statute of the Hans Island in the Kennedy Channel. The fact that it is the only Nordic country that is a member of both NATO and EU shows that Denmark is ***generally supportive of arctic cooperation***. The Danish side, however, considers the Lomonosov Ridge is an extension of Greenland rather than Russia.

Norway

The only Scandinavian country with direct access to the Arctic Ocean, Norway focuses its attention on the issues of ***resource management, environmental impact, and maritime transport***. It is aware of the increased military presence of Russia and *expresses its concern* over the process. Norway focuses on clarifying the status of the "Loop Hole" from the Barents Sea and the "Banana Hole" in the Norwegian Sea.

China

After China became an **observer** in the Arctic Council, Beijing declared China would be an active member in the body. Expanded research was announced, as well as the establishment of a scientific polar institute aimed to explore the complex effects of climate change. China's National Offshore Oil Corporation stated an agreement with Iceland's Eykon Energy firm was signed, to explore Iceland's Southeast coast. Furthermore, China`s interest in exploring resources from Greenland is already well known.

European Union (EU)

With three of its member states being the Arctic States—Sweden, Finland, and Denmark—the European Union claims for a ***permanent observer status*** within the Arctic Council. However, it *firmly opposes* the concept of an "Arctic treaty", stating that "the full implementation of already existing obligations, rather than proposing new instruments should be avoided." Its interest is to keep the balance between the *preservation of Arctic environment* and the need for *sustainable use of potential resources.*

North Atlantic Treaty Organization (NATO)

Considering that five of its member nations—Canada, Denmark, Iceland, Norway, and United States—are part of the Arctic countries, the NATO is *relatively favourable* toward the Arctic Council. One of its goals is to ensure the security and safety of all its members as well as to promote peaceful collaboration among these nations; under NATO, its member states are able to come together for ***collective defence*** if a third party undertakes hostile attacks.

International Action/UN Involvement

United Nations Convention on the Law of the Sea (UNCLOS)

As the only piece of international legislation that currently governs the rights and responsibilities of all states regarding to world seas and oceans, the UNCLOS authorizes ***coastal states to develop and administer special regulations*** dealing with human activities in ice-covered waters. Additionally, it clearly defines *jurisdictional limits* on the ocean area that countries may claim, such as a 12-mile territorial sea and a 200-mile exclusive economic zone limit. Since a potential conflict in the Arctic region may be caused by a territorial conflict, the role of the UNCLOS is crucial.

The Arctic Council

Established in 1996 by the Ottawa Declaration, the Arctic Council is an international ***intergovernmental forum*** with 8 members: United States, Sweden, Russian Federation, Norway, Iceland, Finland, Denmark, and Canada. By providing a means for ***cooperative interaction*** among Arctic States as well as with the Arctic indigenous communities, the council aims to become a "mechanism for addressing the common concerns and the challenges faced by their governments and the people of the Arctic." However, the Arctic Council also explicitly states that it "should not deal with matters related to military security". Some involved actors suggest the Arctic Council should expand its role by adding on its agenda *peace and security issues*, which might become relevant in a close future. According to a survey from 2012, almost two thirds of the interviewed citizens from the Arctic states would definitely agree with the ***idea of an Arctic nuclear-weapons free zone***. Furthermore, a vast majority want the Council to cover peace-building issues. By solving security matters in the Council, the United Nations would not be asked to intervene.

Arctic Monitoring and Assessment Program (AMAP)

Established in 1991 to implement components of the Arctic Environmental Protection Strategy (AEPS), the AMAP is an international organization under the Arctic Council that aims to provide "*reliable and sufficient information on the status of, and threats to, the Arctic environment, and providing scientific advice on actions to be taken in order to support Arctic governments*."

Background information

In 1991, the eight Arctic countries established the ***Arctic Environmental Protection Strategy*** (AEPS), a multilateral, non-binding agreement aimed at Arctic environmental conservation.

Five years later, the ***Ottawa Declaration*** announced the creation of a new intergovernmental forum for Arctic people and governments. Alongside the Arctic states, there are twelve permanent observers in the council. Even though they are not allowed to vote, their participation within the Working Groups is allowed. Important to mention, all the non-Arctic members of the G8 have ***observer status*** in the Arctic Council. Thus, as Damien Degeorges, the founder of the Arctic Policy and Economic Forum, said, "The Arctic has become a *new meeting place* for America, Europe and the Asia Pacific." Presently, the world`s interests are being heated by the melting ice. In 2012, scientists noticed a *record low* of permanent ice in the polar sea; this could possibly be the prediction of an environmental calamity. Nonetheless, these recent events facilitate sea transport and mineral exploitation.

In 2012, the number of transits through the North East Passage (NEP) had increased from 37 to 47 from the previous year. This may not come as a surprise as from Western Europe to East Asia the northern route is around **40 percent shorter** than using the traditional Suez Canal. This is a major advantage for China, where an estimated ***50 percent of its GDP is associated with sea transport***. Moreover, the Russian Federation is interested in exploiting the northern route, as the recent climatic events affect the permafrost and simultaneously the roads and railways. From the resources point of view, according to the US Geological Survey from 2009, around ***15 percent of the undiscovered oil and 30 percent of the undiscovered gas reserves*** in the world are beneath

the Arctic Ocean. As previously mentioned, the United Nations Convention on the Law of the Sea defines the coastal waters as 12 nautical miles off the coast of a state. In other words, even if foreign ships may pass through the territorial waters, it is the state that has sovereignty over the area, as well as to the airspace over and the seabed below. Nil Wang, former Danish admiral and Arctic expert, said that in these regions, more than 97 percent of the discovered energy resources already have an owner. There is a general opinion that the Arctic is "an ungoverned region where all these resources are waiting to be picked up by the one who gets there first. That is completely false". However, he agrees there are some risk factors.

In May 2012 the ***Centre for Climate Change and Energy Solutions*** issued a report, entitled "Climate Change and International Security: the Arctic as a Bellwether". Besides problems like the environmental security, this document tackles as well the remilitarization controversy. "Although the *pursuit of co-operation* is the stated priority, most of the Arctic states have begun to rebuild and modernize their military capabilities in the region. The new military programs have been geared towards combat capabilities that exceed mere constabulary capacity." It is crucial that the delegates understand the relationship between the Arctic states, their stand on the issue and previous disputes. Even if researchers consider there is much scope for cooperation, issues like *oil depletion* and approaches such as 'first come first served' may destabilize the equilibrium. Thus, as many analysts believe, the quest for energy resources may cause a conflict in the region.

Possible solutions/discussion points:

Delegates must realize that the topic is tricky given that the Arctic has undefined territory issues, involves major powers, and has vast untapped resources. Since 1961, the only continent without a native population, Antarctica, has its own treaty, known as the "Antarctic Treaty System". Defining the area as a scientific preserve, the document further authorizes freedom of scientific investigation and ***officially forbids military activities***. The existence of this agreement raised the question of a ***possible Arctic Treaty***, mainly because of the various similarities with Antarctica. ***Clarifying all territorial disputes is essential***. The Article 234 of UNCLOS III, as well as the Guidelines of the International Maritime Organization (IMO) shows the necessity for special *legal instruments in the Arctic*, at the same time, they represent examples of such instruments being established within already existing legal framework. The European Union, however, recommends the implementation of existing treaties, rather than creating new ones.
Delegates must also consider stake issues, whether the Arctic will be international entity and open to all, or confined to the Arctic states, or not exploited at all. The ramifications of all decisions must be considered. The Arctic states need to cooperate to prevent further militarization, and therefore a treaty may provide a medium term solution. Till then, the UN must work with the council to ensure cooperation in the Arctic region.

References

1. *Global warming consequences*
http://nexialinstitute.com/global_flooding.htm

2. *The Exclusive Economic Zone*
http://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm

3. *"The Arctic belongs to Russia"*
http://globalpublicsquare.blogs.cnn.com/2013/07/29/u-s-needs-to-step-up-its-arctic-game/

4. *Creeping militarization of the arctic*
http://thediplomat.com/2013/10/the-creeping-militarization-of-the-arctic/

5. *Arctic prospects*
http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/06/05/warming-up-to-arctic-prospects/

6. *Arctic Environmental Protection Strategy*
http://library.arcticportal.org/1542/

7. *The Arctic Council*
http://www.arctic-council.org/index.php/en/about-us/member-states/111-resources/about/members

8. *Fears of Arctic conflict are 'overblown'*
http://euobserver.com/foreign/119479

9. *Northeast passage*
http://www.martinfrost.ws/htmlfiles/sept2009/northeast-passage-map.jpg

10. *Resources in the Arctic*
http://energy.usgs.gov/RegionalStudies/Arctic.aspx

11. *"Climate Change and International Security: the Arctic as a Bellwether"*
http://www.c2es.org/publications/climate-change-international-arctic-security

12. *A Proposal for an Arctic Nuclear Weapon-Free Zone*
http://interactioncouncil.org/proposal-arctic-nuclear-weapon-free-zone

13. *The United Nations Convention on the Law of the Sea*
http://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm

14. *"Antarctic Treaty System"*
http://www.ats.aq/e/ats.htm

15. *Arctic ownership claims*
http://www.geopoliticalmonitor.com/arctic-ownership-claims