NATO

PACMUN 2016

Director: Jasmine Sun
Chair: Anisha Azad
Assistant Director: Isabella Hedly

PACIFIC MODEL UNITED NATIONS
NORTH ATLANTIC TREATY ORGANIZATION

Dear Delegates,

Welcome to the North Atlantic Treaty Organization at PACMUN 2016! My name is Jasmine Sun, and I am thrilled to be serving as your Director for this conference. I am a senior attending Interlake High School, where this will be my second year of MUN. In addition, I will be joined by my chair, Anisha Azad, and my Assistant Director, Isabella Hedly.

NATO members sit at the heart of many of the world's most pressing security dilemmas. As such, delegates must balance their country's individual perspective with the broader interests of collective security as articulated in Article V. Furthermore, reevaluating the role Western powers and organizations like NATO play is essential given today's changing geopolitical landscape and shift towards multipolarity and global interdependence, as well as an increasingly powerful isolationist movement in internal American politics.

This year, we will be focusing our debates on two particularly fascinating and relevant issues: cybersecurity and responding to terrorist threats in the Middle East.

Given the globalized world's increasing dependence on technology for everything from financial markets to nuclear launches, cybersecurity is more important than ever. The speed of cyberattacks and the difficulty of tracking perpetrators heightens risks of miscalculation; consequently, it is imperative to develop a uniform framework among NATO countries to quickly and effectively deal with cyberthreats before they escalate.

Another issue especially salient in citizens' minds is the threat of terrorism coming from the Middle East. NATO's only invocation of Article V to date was a response to the 9/11 attacks, and as such, there are increasing calls to use it against

terrorism from ISIS as well. However, many still question the prudence of such a drastic measure, and it is up to you all to assess the severity of the terrorist threat and come up with a proportional response.

To ensure substantive, engaged deliberation, I implore you to be thorough and nuanced in your research of your country's stance. Seemingly minor choices in the context of security crises are the difference between escalatory conflict and peaceful negotiations. In fact, the rules of international diplomacy apply just as well to debate: beware of rushing headlong towards conflict, but remember that there can be no progress without confrontation.

I look forward to working with you all, and don't hesitate to reach out if you have questions!

Sincerely,

Jasmine Sun

Director | North Atlantic Treaty Organization

TABLE OF CONTENTS

COMMITTEE INTRO

The North Atlantic Treaty Organization was formed for three main purposes; to curb soviet expansionism, encourage the amalgamation of European politics, and prevent nationalist militarism by creating a powerful North American presence in Europe.[1] The creation of NATO in the aftermath of World War two in 1949 was a historical landmark for the United States as it was first peacetime alliance off the Western Hemisphere ever entered. Starting off as an exchange of the prevention of the spread of communism in Europe in return for economic and military aid from the US, NATO has become one of the most strongest and influential alliances in the world.[2] The 2010 strategic concepts defines NATO's goals the attainment of cooperative security, collective defense and crisis management.

NATO is unique in that it safeguards its member states by considering any attack towards one of its members as an attacks towards all of its members. This act of taking care of its members has been coined "collective defence" and has only been invoked once as a response to the 9/11 terrorist attacks in the United States, beginning the campaign against international terrorism. In addition, unlike UN committees, NATO possesses the power to make security decisions in any means and level with a consensus of all 28 member nations. Consequently, NATO assumes an extremely active role in crisis-management missions and civil emergency operations globally.[3]

NATO's has two components of its protection; political and military. The political side advocates for democratic values and stresses the importance of cooperation in order prevent conflict. This political component can be seen in current actions in Afghanistan where NATO is providing training and assistance to Afghan security forces.[4]The military side can undertake crisis operations if a diplomatic resolution can't be met. The bombing of Yugoslavia in 1999 is an example of a militaristic approach mandated by the U.N.'s Secretary General Kofi Annan to prevent further ethnic cleansing genocide that peaceful solutions couldn't resolve.[5] NATO's founding treaty, Article 5 of the Washington treaty, states all military operations must be completed consensually through the cooperation of countries and international organizations.

1 http://www.nato.int/history/nato-history.html

2 https://history.state.gov/milestones/1945-1952/nato

3 http://www.nato.int/nato-welcome/index.html#basic

4 http://www.natolibguides.info/transition-

5 http://www.history.com/topics/cold-war/formation-of-nato-and-warsaw-pact/videos/nato-offers-aid-to-united-states-following-911-attacks

TOPIC 1

CYBERSECURITY

TOPIC INTRO

As technological development accelerates, the world simultaneously becomes increasingly dependent on technology for its military operations, critical infrastructure, and commerce.[6] Consequently, cyberattacks, which compromise computer networks and other technological infrastructures, have become increasingly common. Their allure as an alternative to kinetic warfare can be attributed to both the low resource expenditures required to execute an attack as well as the difficulty of tracking attackers, factors which even the battlefield between large state and small non-state actors. Furthermore, cyberattacks occur with instant effects, requiring rapid decision-making by states and involving a higher risk of miscalculation.[7] In fact, the United States FBI ranked cyberwar as the third greatest threat to national security after nuclear war and WMDs, and the 2007 cyber-attacks on Estonia's critical infrastructure resulted in casualties and damage comparable to a conventional attack. [8]

Therefore, it is critical that nations strengthen their cyberdefense systems to both prevent and effectively respond to such attacks, which are often highly unpredictable. Nations tend to adopt one of two primary security strategies: *cyberdeterrence* and *cyberdefense*. A cyberdeterrence strategy follows the same logic of nuclear deterrence and involves building up a nation's own array of cyberweapons to intimidate and discourage potential attackers for fear of retaliation.[9] On the other hand, cyberdefense prioritizes securing and defending a nation's systems through measures such as closing software backdoors, disclosing zero-day flaws, and ending other surveillance mechanisms that create vulnerabilities for attackers to exploit.[10]

NATO's primary roles regarding cybersecurity include protecting its own information systems and coordinating cybersecurity cooperation among member states. Other key initiatives include expanding communication with industry about threats and increasing general awareness of the dangerous potential of cyberwar.[11] Although no NATO country has yet experienced a cyberattack deadly enough to necessitate a coordinated offensive response, NATO did provide Estonia with

6 Kshetri, The Global Cyber-crime Industry, 2007.

7 Clarke, Cyber War, 2010.

8 Kshetri, The Global Cyber-crime Industry, 2007.

9 Libicki, Brandishing Cyberattack Capabilities, 2013.

10 Masnick, "National Insecurity," 2013.

11 NATO "Cyber defence," 2014.

technological assistance to aid recovery from the 2007 attacks, which shut down government websites, online banking, and online media publications for weeks.[12] In addition, NATO notably updated Article V in its 2014 charter to expand collective defense to cyberattacks against member nations.[13] However, there remain significant concerns regarding NATO's cybersecurity strategy. In particular, questions have been raised about the effectiveness of Article V deterrence given the difficulty of identifying attackers in cyberspace, and NATO's planned response to a more devastating attack remains unclear.

HISTORY

Cybersecurity is primarily a modern-day concern, since only recently have businesses and governments utilized cyberspace-based technology to manage and conduct daily operations. However, since the first computer worm in the 1980s, cyberattackers have orchestrated attacks with the capacity to not only steal unclassified information from personal computers, but also put nuclear power plants[14] and military assets[15] at risk. Therefore, in parallel with the escalating danger of cyberattacks, nations have found it increasingly necessary to develop a comprehensive cybersecurity strategy.

The Morris computer worm is widely considered the first major computer worm - a piece of malicious code that self-replicates to spread harm.[16] In 1988, the worm disabled ten percent of Internet-connected computers in the United States and cost hundreds of thousands in damages. Previously, the Internet community - which was limited to mostly academics, rather than businesses and everyday users - was not aware of the destructive capacity of viruses.[17] However, the rapid and widespread effect of the Morris worm effectively ignited these fears, jumpstarting the cybersecurity industry and leading to the establishment of Computer Emergency Response Teams to develop rapid solutions to these crises.[18] Still, a key difference remains between the Morris worm and other major attacks: while Robert Morris, the creator of the worm, did not intend to cause an infection of such massive scale, other attackers are usually far more malicious and targeted in their attacks. For example, the ILOVEYOU and Melissa computer viruses infected millions of personal computers throughout the 1990s via email attachments, prompting the development of antivirus software.[19]

12 Wolff, "NATO's Empty Cybersecurity Gesture," 2014.

13 Risen, "Cybersecurity Remains a Gray Area for NATO," 2014.

14 http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

15 http://www.eweek.com/c/a/Security/Defense-Department-Confirms-Critical-Cyber-Attack-551206

16 http://www.pctools.com/security-news/what-is-a-computer-worm/

17 http://www.intelfreepress.com/news/lessons-from-the-first-computer-virus-the-morris-worm/7223/

18 http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

19 Ibid.

In the 2000s, however, cyberattacks shifted focus from personal computers onto stealing information from or compromising the systems of businesses and governments. These attacks were often waged as a result of political motives.

State actors and political organizations are the primary agents conducting politically motivated cyberattacks. The 2007 cyberattacks on Estonia are the first instance of international cyberwarfare. In this situation, DDoS cyberattacks on the technology infrastructure of the Estonian government, universities, TV and newspaper organizations, and financial institutions shut down much of the country's online operations for three weeks.[20] Although an IP address traced to a member of the Russian government suggested Russia was to blame, the Estonian government could not determine who the specific attackers were, and as such only made one arrest.[21] This is known as the attribution problem, or the difficulty of identifying attackers due to the anonymity of the Internet. Since 2007, Estonia has invested heavily in cybersecurity by developing departments to carry out risk assessments of information systems, monitor and respond to attacks on government websites, and develop an IT partnership between the public and private sector.[22]

In another instance, Stuxnet was an immensely advanced worm that targeted and destroyed one-fifth of Iranian nuclear centrifuges in 2010. The attack was orchestrated by the United States and Israel in order to hinder Iran's uranium enrichment programs, and reportedly delayed them by several years.[23] Meanwhile, Russian officials have condemned the riskiness of such endeavors, suggesting that Stuxnet had the potential to trigger a nuclear meltdown with devastating long-term health and environmental effects.[24] Consequently, Stuxnet served as a major warning of the escalatory potential of cyberwarfare.

PAST NATO ACTION

NATO's involvement in cybersecurity has been a fairly recent phenomenon, as it instituted its first cyber defence policy in 2008 in response to the 2007 cyberattacks on Estonia.[25] In 2014, NATO updated its charter to include cyberwarfare under the Article V provision, which states that an attack on one member nation constitutes an attack on all.[26] Since then, NATO has continued to develop and invest in programs for collective cybersecurity.

20 http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-aga inst-cyberwarfare

21 http://www.iar-gwu.org/node/65

22 https://e-estonia.com/the-story/digital-society/cyber-security/

23 http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

24 http://www.telegraph.co.uk/news/worldnews/europe/russia/8262853/Stuxnet-virus-attack-Russia-warns- of -Iranian-Chernobyl.html

25 http://www.nato.int/cps/en/natohq/topics_78170.htm

26 http://www.usnews.com/news/articles/2014/08/14/cybersecurity-remains-a-gray-area-for-nato

At the time of the cyberattacks on Estonia's public and private sector online infrastructure in 2007, NATO policy on cybersecurity was still virtually nonexistent, having been only mentioned briefly at the 2002 and 2006 summits.[27] In fact, the lack of clarity surrounding whether cyberattacks were legitimate threats to national security meant that Estonia was reluctant to invoke Article V and consequently failed initially to secure allied aid.[28] Soon after, however, NATO helped Estonia by sending cyberterrorism experts to expedite and guide recuperation efforts. In fact, NATO developed its first Policy on Cyber Defence in January of 2008, indicating that NATO would "provide a capability to assist allied nations, upon request, to counter a cyber attack" in situations like that of Estonia.[29] Furthermore, Estonia today is often regarded as a model for a strong cybersecurity framework, and is home to the NATO Cooperative Cyber Defence Center of Excellence (CCDCoE) that was established after the attacks.[30] The CCDCoE serves as a research and training facility that coordinates cybersecurity training and information between NATO member states, the private sector, and academic experts.[31] Its five branches focus on the topic areas of Law and Policy, Cybersecurity Strategy, Technology, Education and Exercise, and Support.[32]

A focus on a cybersecurity strategy was reaffirmed at NATO's 2010 Lisbon Summit's Strategic Concept, which explicitly stated plans to develop cyber defence capabilities utilizing the NATO planning process.[33] These plans were developed further in the second NATO Policy on Cyber Defence in June 2011, which had the principal focus of protecting NATO's communication networks by mandating requirements for the security of its information systems, implementing early warning and awareness capabilities, and integrating cyber defence into the NATO Defence Planning Process.[34] To fulfill these goals, in October 2013, NATO invested 58 million Euros (65.2 million USD) into the NATO Computer Incident Response Capability (NCIRC) to protect NATO information systems in response to a growing number of cyberattacks on its networks. This program includes services spanning preventative measures, responsive measures, and legislative support.[35]

Because governments of many member states are so dependent on external contractors to manage their information systems, public-private sector cooperation has become a key component of NATO's cybersecurity strategy. These efforts were initiated in September 2014 with the launch of the NATO Industry Cyber Partnership

27 http://www.nato.int/cps/en/natohq/topics_78170.htm

28 http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-aga inst-cyberwarfare

29 http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=33636

30 https://e-estonia.com/the-story/digital-society/cyber-security/

31 https://ccdcoe.org/about-us.html

32 https://ccdcoe.org/structure-0.html

33 http://www.nato.int/cps/en/natohq/official_texts_68580.htm

34 http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

35 https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf

(NICP) in collaboration with 1,500 industry leaders and policymakers.[36] The objectives of the NICP include improving supply chain security, engaging in information exchange, share best practices in cybersecurity prevention and recovery, and cooperate in education and training. Although similar programs were already in place in countries like Estonia and the Netherlands, the NICP centralized efforts while encouraging other countries to model such systems.[37] NATO continues to expand partnerships with both private sector actors and other international organizations in the present day.

CURRENT SITUATION

In the modern day, cyberthreats are increasingly common because of an increasing dependence on technology for economic and political infrastructure, a risk exacerbated by the gap in communication between the public and private sector.[38]

For example, more importantly than the immediate consequences of the Stuxnet attack, it revealed a major weak point in the cyberspace: in order to compromise nuclear energy infrastructure, the worm first exploited zero-day flaws (vulnerabilities unknown to the software vendor) in the Windows OS.[39] Oftentimes, even though the companies do not know the zero days exist, the government does - and is actively stockpiling the vulnerabilities for their own use as a means of national surveillance and offensive cyber operations.[40] In fact, the United States government is the biggest buyer and thus the lynchpin of the global zero-days market, ensuring that the software worldwide will remain vulnerable to cyberattacks as long as there continues to be government demand.[41] This lack of transparency between the public and private sector has spurred massive outrage from cybersecurity advocates, who demand full disclosure.[42]

The most common recent cyberattacks have had mostly economic motives and are designed to steal business and personal information from businesses. In fact, over one-fifth of manufacturing companies in 27 surveyed countries reported losing intellectual property to cyberattackers in 2014.[43] As a result of the theft of trade secrets, countries' GDPs are suffering -- estimates suggest that the United Kingdom's GDP suffers by 1% for every 1% increase in IP crime[44] -- as well as their military and economic

36 http://www.nato.int/cps/en/natohq/topics_78170.htm

37 https://www.ncia.nato.int/NewsRoom/Pages/140918-NATO-launches-Industry-Cyber-Partnership.aspx

38 http://phys.org/news/2014-08-deter-cyberattacks-public-private-partnership.html

39 http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

40 https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabi lities

41 http://in.reuters.com/article/usa-cyberweapons-idINDEE9490AX20130510?type=economicNews

42 https://www.eff.org/press/releases/eff-sues-nsa-director-national-intelligence-zero-day-disclosure-process

43 http://www.computerweekly.com/news/2240226840/IP-theft-hit-21-of-manufacturers-in-past-year-study-sh ows

44 Ibid.

competitiveness.[45] However, cyberattacks on corporations is not limited to stealing IP. In 2014, a wave of Chinese and Russian-origin cyberattacks stole payment card data from tens of millions of customers whose information was stored in corporate databases. These security breaches affected many major businesses including Target, Home Depot, Neiman Marcus, and JP Morgan Chase, illuminating the inadequacy of cybersecurity systems in even the most modern companies. Although the attacks targeted United States firms, infected networks in one country can easily affect others, highlighting the need for continued international cybersecurity cooperation.[46]

Additionally, in 2016, NATO established a partnership between the NCIRC and the Computer Emergency Response Team of the European Union (CERT-EU) to pledge cooperation to information sharing between the two organizations.[47] Sure to affect this arrangement, however, is Britain's choice to leave the European Union. Although the EU is ratcheting up its current cybersecurity policy in order to create clear international regulatory frameworks such as the EU-US Privacy Shield, these moves towards regulatory clarity and uniformity are put at risk by Britain's departure. It remains unclear to what extent Britain will adhere to the EU's data protection standards and continue the collaboration key to international cyberdefense.[48]

BLOC POSITIONS

UNITED STATES/WESTERN BLOC

In 2013, the United States dealt with the largest breach of information in its history as Edward Snowden copied and leaked sensitive information from the FBI and leaked it worldwide. Consequently, the United States spent years trying to catch Snowden, limit the damage done from the leak of information, and then prevent future issues by tightening up their cyber security. However, while the United States was trying to recuperate from this information breach, they also faced increasing issues of cyberthreats such as having their politicians' private information stolen, military plans leaked, and cybersecurity threats from terrorist groups.

As a result of the cybersecurity threats the United States was dealing with, the country came up with more effective ways of dealing with cybersecurity. The first step the United States uses is sending information about imminent threats to a branch of the Federal Bureau of Investigation (FBI) that is set up to deal with cybersecurity threats which was formed after the Snowden leak in 2013. Once this branch is alerted of the threat, they track where the threat came from and they evaluate the validity of the threat before seeking punishment or retribution for attackers. If found, these

45 https://washingtontechnology.com/articles/2011/07/21/stan-sloane-cyberattacks-ip-threats.aspx

46 http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

47 http://www.nato.int/cps/en/natohq/news_127836.htm

48 https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective

people are then tried in the judicial system and often imprisoned for their actions. It is only in very rare cases when the security of large masses is at risk or when the threats come from known terrorist groups that the government utilizes military personnel to shut down the threats.

Because the United States focuses on taking out the people behind the cyber security threats, it is likely that the United States would support using technology or nonviolent groups to combat cybersecurity threats. This technology includes mass surveillance techniques as well as offensive cyber operations, such as the stockpiling of zero day vulnerabilities. However, despite government-led technological initiatives, the Department of Defense remains opaque about its cyber capabilities with regards to the private sector and general populace -- a decision contrasting with the transparency-oriented policies of many European nations.

UNITED KINGDOM

The United Kingdom is currently one of the highest ranked countries worldwide for how effectively they deal with cybersecurity breaches and threats. This is because the government has a branch called the Office of CyberSecurity and Information Assurance which works solely to ensure the cybersecurity of all of its citizens. When this group finds a cybersecurity threat or breach, the group has a defined protocol for dealing with and eliminating the threat. Because the group is constituted of the nation's leading cybersecurity experts, when a threat is found the group can work quickly to attribute the threat and implement consequences. This process avoids military involvement, and the military is only used when there are extreme threats to safety or when it is difficult to find and detain perpetrators.

However, in general, the United Kingdom deals with cybersecurity via preventative measures that avoid threats in the first place. The government implements stringent security measures and educates the public on how they can prevent threats. Even schoolchildren are involved in education measures, as it is crucial that the younger generation is prepared to deal with an increasingly common security problem. The government set up programs that help companies teach their employees cyberresponse and online safety techniques. All these programs help to avoid threats because the public is educated and there are groups set up to deal with any threats that might show up.

Overall, from the education measures and non-violent measures for dealing with cybersecurity threats, it is clear that the United Kingdom would likely support dealing with cybersecurity threats by setting up government task forces to deal with threats in a nonviolent way.

EUROPEAN BLOC

All of the European countries have dealt with cybersecurity threats and breaches in various forms. As a result of this common threat to their collective security, many European countries banded together to form the European Cyber Security Organization (ECSO) in June 2016, an international nonprofit organization, in order to deal with cybersecurity threats. The ECSO is an "industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership."

Within this organization, all of the countries can call upon each other when dealing with large cybersecurity threats in order to shut down the threats safely. As a result, the countries can encourage cooperation between each country's brightest cybersecurity technicians to backtrack and attribute threats. This me.ans that the threats can be taken down as easily as possible, avoiding the need for military involvement.

The ECSO is also unique in that it favors a market-based approach to reducing cyberthreats by sponsoring Research and Innovation while facilitating market intake of new solutions. It favors taking advantage of free trade agreements such as the EEA and EFTA to foster information exchange -- a position which is likely to conflict with Britain's post-Brexit protectionist administration. Furthermore, the focus of the ECSO on public-private partnerships contrasts with the lack of transparency between the public and private sectors in nations like the United States.

With the cooperation of these countries, most of them would support organizations to deal with cybersecurity threats but they would not support military actions as these countries support cooperation over the damage of military.

CASE STUDIES

2007 CYBER-ATTACKS IN ESTONIA

The 2007 cyber-attacks in Estonia, which downed government and business computer networks across the country, are often regarded as the world's first act of cyberwarfare. These took the form of DDoS attacks, which swamped websites in order to jam and prevent normal users from accessing them for three weeks.[49]

Because the attacks occurred at a time of political tension between Estonia and Russia, the Estonian government immediately blamed the Kremlin. However, both Estonian officials as well as NATO later admitted they had no concrete evidence

49 http://www.csmonitor.com/2007/0517/p99s01-duts.html

linking the attacks to the Russian government.[50] This inability to identify the perpetrator of the attacks is often discussed as the "attribution problem" regarding cyber-warfare, an issue that heightens the probability of miscalculation and preemptive attacks between states conducting brinksmanship.[51]

The short-term consequences of the attacks were far-reaching, as the country was ill-equipped to deal with cyber-attacks of such a scale and intensity. Institutions targeted by the attacks included government, media, financial services, and business networks, consequently temporarily shutting down Estonia's economy and communications with the outside world. Not only were the attacks wide in scope, but they were effective primarily because of the highly methodical and discreet planning utilized by the attackers. For example, botnets (computers controlled by outsiders to infect other networks) from over 50 countries were used, making it more difficult to isolate and quarantine them.[52]

Fortunately, after three weeks, the attacks stopped, allowing the recuperation process to begin. Because NATO had not yet clarified whether cyber-war constituted an act of war, and therefore Article V could not be mobilized, the NATO countries did not initiate an offensive response. However, they did send several cyber-terrorism experts to Estonia to assist recovery efforts and establish the Co-operative Cyber Defense Center of Excellence in Tallinn, which to this day is a key agent in conducting cyber-defense research and developing international responses to cyber-threats.[53]

STUXNET

Stuxnet is a malicious computer worm believed to have been developed by the American and Israeli governments in order to sabotage Iran's nuclear enrichment program.[54] It took advantage of zero-day vulnerabilities, or undisclosed software flaws, to attack Windows operating systems in the centrifuges' central control centers.

The great technological complexity of Stuxnet suggests it had been in development for years. Anonymously reporting American officials remarked that the cyber-weapon was originally sanctioned by the George W. Bush Administration to damage both the capability and confidence of Iran's nuclear program by creating a series of "accidents" at nuclear facilities.[55]

Although Stuxnet spread -- likely unintentionally -- to countries other than Iran as well, only the specific set of processes present in a nuclear centrifuge would trigger

50 http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack

51 http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/

52 http://www.iar-gwu.org/node/65

53 Ibid.

54 https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-offic_ials-say/2012/06/01/gJQAlnEy6U_story.html

55 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

the cyber-weapon, causing plants to self-destruct. However, in spite of its advanced programming, the weapon achieved only limited success, destroying one-fifth of Iran's nuclear centrifuges.[56] By the end of the year, in fact, Iran began installing new centrifuges, reaching close to the original 6,000 by the following February.[57]

The most significant implication of the Stuxnet attack was its role in revealing the destructive power of offensive cyber-weapons. In the case of the Iranian nuclear plants, a more disastrous meltdown could have had catastrophic effects similar to those caused by the Chernobyl disaster.[58] This risk is exacerbated by the fact that public critical infrastructure like the water supply, electricity grid, and even military command and control are all hooked up to systems vulnerable to attacks like Stuxnet.[59]

GUIDING QUESTIONS

- How can NATO work with non-member countries to prevent cyberattacks?
- How can countries balance domestic surveillance needs with risks to national security?
- What mechanisms can be used to create better channels of communication between the public and private sector?
- How can countries effectively respond to cyberattacks with unknown perpetrators?
- How can countries better secure their critical infrastructure?
- How can NATO differentiate acts of cyberwar from generalized, everyday cyberattacks?

FURTHER RESEARCH

Brief history of international cyber-threats:

- http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

Summary of NATO cyber defense policy:

- http://www.nato.int/cps/en/natohq/topics_78170.htm

56 http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

57 https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

58 http://www.csmonitor.com/World/Latest-News-Wires/2011/0131/Stuxnet-virus-penetrates-nuclear-plant -may-cause-Chernobyl-like-disaster

59 http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Explanation/history of zero day vulnerabilities and stockpiling controversy:

- https://www.wired.com/2014/11/what-is-a-zero-day/

Case studies:

- Overview of Estonian attacks:
  http://www.iar-gwu.org/node/65
- Stuxnet:
  https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

TOPIC 2

RESPONDING TO TERRORISM IN THE MIDDLE EAST

TOPIC INTRO

ISIS or The Islamic State of Iraq and the Levant is a jihadist militant group that is responsible for countless deaths and thousands upon thousands of injuries in most countries of the world. Based out of Iraq and Syria, this group follows an Islamic fundamentalist Wahhabi doctrine as they try and claim religious, political, and military authority over all Muslims worldwide. Since their rise to worldwide terror in June of 2014, the group has claimed responsibility on hundreds of attacks around the world from the recent Paris attacks in January 2016 to attacks at a hotel in British Territory in June 2015.

With attacks increasing in intensity every month and countless numbers of men, women, and children being tortured, beaten, maimed, injured, and murdered, the importance of stopping ISIS has been recognized by countries around the world and brought to the attention of NATO.

Combating ISIS and other militant groups is not a new subject for countries to deal with and for NATO; in 2001 NATO invoked its collective defense clause for the first and only time in response to the terrorist attacks on the United States in order to take out Al Qaeda. This was one of the first time that multiple countries banned together to fight. "war on terror" in order to take out the group responsible for taking the lives of thousands of innocent people. The United States was the main group to end this war when they killed the leader of the group, but Al Qaeda would not have been taken down without the help of other countries. However, in order to take down this militant group there was an entire war fought on the ground and thousands of innocent lives were lost in order to keep other lives safe. It is because of this that groups are more hesitant now to engage in an actual war on ISIS.

Currently, ISIS is growing stronger in power as they recruit more young children to fight for their cause and die as martyrs. This gain in strength worries the leaders of major countries as they all wonder who will be the next victim in ISIS's game of terrorist attacks. However, the opinions on how to combat ISIS are mixed as there are different viewpoints on how to stop ISIS and there are different viewpoints on the importance on combating ISIS. The most popular opinion and most commonly published opinion current is that of a "war on terror." This would involve an actual war fought by soldiers using weapons in order to kill the members of ISIS. The theory is that if this "war on terror" worked to stop Al Qaeda, then it should stop ISIS. This viewpoint is shared among the more powerful countries, those who make money off of war, as they believe that a physical war should be fought to stop ISIS. They believe

that bombing ISIS's locations and putting the lives of soldiers on the lines to engage in hand-to-hand combat in order to kill ISIS soldiers is the best way to deal with ISIS. Meanwhile, there are other countries who believe that the best way to combat ISIS is by dealing diplomatically and trying to cut off the supply of weapons for ISIS and to focus more on minimizing the effects of terrorists' attacks rather than trying to take out the members of ISIS. Furthermore, there are the countries that believe that ISIS is not of main importance of NATO as NATO should be focusing more energy on the United States and Russia relationship of the issue with Syrian relations and their refugees. All of these probe the idea of whether a "war on terror" is really the way to go in combating ISIS.

HISTORY

Terror Threats in the Middle East are primarily a modern-day concern, as it has only been in the past few decades with new military advancements that terrorist groups have gained considerable prominence and influence on the world stage. Terrorist groups first gained control of areas in the Middle East in the 1980's after the military advancements of the Cold War, including the invention of automatic and nuclear weapons. These made the existence of extremist groups considerably more dangerous, since they could potentially have destructive capability similar to powerful nation-states. However, it was not until the terrorist attacks in 2001 on the United States that NATO developed a unified response to terrorism.

The attack on America in September of 2001 is one of the first instances of NATO responding to terrorist threats in the Middle East. In fact, NATO invoked its collective defense clause for the first and last time to date in response to the 9/11 terrorist attacks, which were perpetrated by the terrorist group Al Qaeda. The member states united to focus on awareness, capabilities, and engagement to combat Al Qaeda and prevent future attacks. For example, the international community and the G8 in particular implemented domestic legislation to prevent attacks, financing terrorists, and prosecute them. However, while all member states cooperated, America was one of the most active member states because they engaged in ground combat in countries where Al Qaeda was known to be based such as Iraq and Syria.

In 2015, with the rise of the terrorist group ISIS and the attacks on Paris, Britain, as well as on numerous civilian populations in Iraq and Iran, NATO member states banded together to combat ISIS. Within in this time period, numerous civilian groups and member states such as Anonymous and the United States declared war on ISIS.

PAST NATO ACTION

Since NATO first identified terrorism as a threat to its collective security in its 1999 Strategic Concept,[60] combatting terrorism has been one of its primary and most active roles.

The 9/11 attacks on the World Trade Center in New York City catalyzed a series of counter-terrorism initiatives. In fact, it is the only incident to date in which NATO has invoked Article V of the Washington Treaty, commonly known as the "collective defence clause." Consequently, within a month of the attacks, NATO countries agree on a package of responses to prevent further terrorism through measures such as intelligence-sharing and military assistance from other NATO countries to the United States. Furthermore, Operation Eagle Assist and Operation Active Endeavor utilize NATO military assets to patrol the United States and Eastern Mediterranean for threats.[61]

At the Prague Summit in 2002, NATO reaffirms their dedication to counter-terrorism through a new commitment package, involving heightened international cooperation, as well as expanding defense to the missile and cyber realms.[62] One new program emerging from the Prague Summit is the Partnership Action Plan against Terrorism, which emphasized human rights concerns and outlined a framework for broader cooperation through political consultation.[63] In addition, in 2002, NATO created the NATO Response Force to streamline military command, especially in the context of counter-terrorism.[64]

As technology developed, so did terrorist arsenals, which began to incorporate advanced weapons such as bioweapons, chemical weapons, radiological weapons, and even nuclear WMDs. Therefore, in 2003, NATO created the NATO Combined Joint Chemical, Biological, Radiological, and Nuclear (CBRN) Defence Task Force to counter these new threats. While the CBRN Defence Battalion focuses on military readiness, the Joint Assessment Team conducts threat evaluations.[65]

CURRENT SITUATION

The primary terrorist threat in the Middle East today is that of ISIS, or The Islamic State of Iraq and Syria, which gained worldwide recognition in early 2014 as a result of its Iraqi offensive, which included incidents such as the Sinjar Massacre and

60 http://www.nato.int/cps/en/natohq/topics_77646.htm

61 Ibid.

62 Ibid.

63 http://www.nato.int/cps/en/natolive/topics_50084.htm

64 www.nato.int/cps/en/natolive/topics_49755.htm

65 http://www.nato.int/cps/en/natohq/topics_49156.htm

capture of Mosul.[66] Currently, several NATO countries are combatting ISIS, whether through targeted drone strikes or sending in troops.

Current NATO initiatives to counter increasing terrorism in Iraq, largely stemming from ISIS, include training of Iraqi forces[67] and coordinate airstrikes, such as the United States has supported in a recent anti-ISIS coalition.[68] In fact, the US has conducted over three-quarters of total airstrikes up to October 31, 2015, the majority of which were directed at Iraq.[69] In addition to the US, France has also pushed for greater NATO participation -- and even potential invocation of the Article V collective defence clause -- in response to recent attacks, such as the Paris attack in 2015. However, non-NATO players are also significant in combatting ISIS; for example, the Iranian government has advised militias while Kurdish and Yazidi fighters have engaged in ground combat.[70]

One recent development that is especially salient is Britain's planned exit from the European Union. Jens Stolberg, the Secretary General of NATO, indicated that Brexit could severely endanger the ability of NATO to provide a united force against terrorism. This is especially because the UK provides the most forces to NATO among the European allies and bridges the United States and Europe.[71]

BLOC POSITIONS

EUROPEAN BLOC

Terrorist groups such as ISIS have affected all countries within Europe in some form or another. France, for example, lost numerous citizens in a major 2015 attack from ISIS on Paris, while other countries like the United Kingdom lost citizens in attacks on British Territory. Even countries that did not suffer from direct attacks experienced related issues such as threats or refugee inflows from destabilized regions such as Syria. Because many of these countries are facing threats, European governments must manage dilemmas such as the desire to mitigate terrorism via hardline positions like airstrikes and anti-radicalization programs versus programs designed to promote social harmony that may alienate right-wing parties. However, as these nativist political factions gain popularity domestically, European governments are increasingly capitulating to pressures to abandon neutrality and engage terrorists directly in combat. Recently, Belgium has conducted raids in order to defuse threats of

66 http://www.cnn.com/2014/06/23/world/meast/iraq-crisis/

67 http://www.atlanticcouncil.org/blogs/natosource/jens-stoltenberg-nato-s-role-in-fighting-terrorism

68 http://time.com/3273185/isis-us-nato/

69 http://www.cnn.com/2015/11/20/world/war-on-isis-whos-doing-what/index.html

70 Ibid.

71 https://www.theguardian.com/world/2016/jun/22/nato-chief-says-uk-staying-in-the-eu-is-key-to-fighting-ter rorism

terrorist sleeper cells in Germany, Belgium, and the Netherlands. France has also announced new airstrikes on Raqqa, Syria.

NORTH AMERICAN BLOC

On September 11th, 2001, the United States received the worst terrorist attack on American soil when Al Qaeda crashed planes into the Twin Towers, killing over a thousand people. After this attack, the United States declared a "war on terror" as they sent troops in Afghanistan and Iraq to search for and destroy the Al Qaeda leadership. As a result of these initiatives, the United States took out Osama Bin Laden as well as other leaders of Al Qaeda.

As other terrorist groups like ISIS rose to power, the United States continued the War on Terror. US-supported counter-terrorist strategies involve both deployment of troops into ground combat and missile airstrikes, which are increasingly appealing because of the relative security for American lives. Given these previous actions and the fact that the United States economy improves during wartime, it is more likely to support direct combat tactics to solve terrorism in the Middle East.

Canada has empirically supported US counterterrorism efforts, as the two countries are long-time allies. Beginning in 2014, Canada began to approve air combat missions against ISIS. Canadian citizens have also joined terrorist groups, feeding into radicalization programs that also affect the United States and Europe. Like the United States, Canada, however, has not yet sought to severely limit or ban refugees from the Middle East as a result of terrorist fears.

CASE STUDIES

SINJAR MASSACRE

The Sinjar Massacre was the murder of thousands of Yazidi men by the Islamic State of Iraq and the Levant in Sinjar City, Iraq in August 2014. ISIS militants attacked the city of Sinjar, causing tens of thousands of Yazidis, the resident religious minority group, to flee to the Sinjar Mountains, where ISIS conducted a siege.[72]

The attack occurred only two months after the launch of ISIS's Northern Iraq Offensive against the Iraqi government, in which ISIS declared themselves as a new Islamic caliphate. While the United Nations described the intentions of the massacre as motivated by genocidal intent,[73] Kurdish officials cited the geographically strategic location of Sinjar as being key to ISIS's Arabization campaign instead. Furthermore, ISIS aimed to humiliate the Kurdish state, which they accomplished by selling

72 http://www.huffingtonpost.com/mark-hetfield/massacre-at-sinjar-has-th_b_7936750.html

73 http://europe.newsweek.com/one-year-sinjar-massacre-yazidis-blast-lack-action-over-hostages-331216?rx =us

thousands of Yazidi women into sex slavery while others were forcibly converted to Islam.[74]

The immediate consequences of the attack were the deaths of 5,000 Yazidi men at the hands of militants as well as more violence from starvation, abductions, and displacement from their homes. Many held in activity were broken up from their families or forced to training camps to learn to fight for ISIS. In fact, Sinjar became uninhabitable due to ISIS occupation, triggering waves constituting up to 350,000 Yazidi refugees fleeing from northern Iraq.[75]

In order to deal with the massacre as well as ISIS's expansion across northern Iraq more broadly, countries such as the United States, France, and the United Kingdom responded with air drops of food, water, and medicine.[76] Coupled with the humanitarian offerings, however, were a series of US-led military drone strikes on the Sinjar region as part of a "long-term project" of protecting civilians from terrorism.[77] Therefore, events such as the Sinjar massacre spurred the broader question of to what extent Western countries should involve themselves in world affairs in the Middle East.

2010 PALESTINIAN MILITANCY CAMPAIGN

In response to the projected commencement of peace talks between Israel and the Palestinian authority in 2010, a coalition of 13 Palestinian militant groups led by Hamas organized a series of terrorist attacks to derail negotiations. The attacks largely took the form of shootings and rocket attacks along the West Bank of Israel.[78]

The 2010 peace talks were a hopeful end to a decades-long military conflict over territorial claims between Palestine and Israel, coordinated with the aid of US President Obama, Israeli President Netanyahu, and Palestinian Authority Chairman Abbas.[79] However, Palestine militant groups including Hamas and the Popular Resistance Committees have expressed discontent with the planned negotiations, insisting that the talks would inevitably cede too much land to Israel and that armed conflict was the only way towards Palestinian liberation.[80]

74 http://rudaw.net/mobile/english/interview/29122014

75 http://www.telegraph.co.uk/news/worldnews/islamic-state/11160906/Isil-carried-out-massacres-and-mas s-sexual-enslavement-of-Yazidis-UN-confirms.html

76 http://abcnews.go.com/International/obama-authorizes-air-strikes-iraq/story?id=24884633

77 http://www.businessinsider.com/military-air-strikes-2014-8

78 http://www.irishtimes.com/news/islamist-groups-attempt-to-derail-middle-east-talks-1.646680

79 https://www.theguardian.com/commentisfree/2010/apr/26/israeli-palestinian-peace-talks

80 http://www.memri.org/report/en/0/0/0/0/0/0/4628.htm

Shootings primarily targeted Israeli civilians, who were branded by the Palestinian resistance as "illegal settlers" on their land. Militant leaders utilized the attacks on ordinary Israelis in order to weaken the Palestinian negotiating position in the talks and consequently demonstrate their futility.[81] Hamas also increased rocket attacks from the Gaza Strip during this time, which are aimed mostly at causing psychological trauma among the Israeli populace rather than upping the death count.[82]

Although it is not entirely clear to what extent the militancy campaign was effective, the peace talks collapsed in late September when the moratorium on settlement expired because the Palestinian Authority refused to recognize the Jewish State.[83] Since then, hostilities have continued.

GUIDING QUESTIONS

- How can countries reconcile the need to target terrorists with risks to civilians?
- What non-military tactics can NATO use to decrease the risk of terrorism in the Middle East?
- How can NATO countries cope with the influx of refugees from terrorism-impacted areas?
- How can countries prevent their interventionism from exacerbating anti-Westernism?
- How effective is mass surveillance as a strategy of preventing terrorist threats? To what extent can it be reconciled with infringements on personal privacy?
- How can NATO member countries split the resource burden of fighting terrorism?
- How can countries assess the necessity of interventionism to resolve regional terrorism?

81 http://www.washingtonpost.com/wp-dyn/content/article/2010/09/06/AR2010090602958.html

82 http://news.bbc.co.uk/2/hi/middle_east/7270168.stm

83 http://www.haaretz.com/israel-news/netanyahu-offers-settlement-freeze-in-return-for-recognition-as-jewish -state-palestinians-say-no-1.318447

FURTHER RESEARCH

Brief history of terrorism in the Middle East:

- http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/modern.html

Overview of NATO counter-terrorism policy:

- http://www.nato.int/cps/en/natohq/topics_77646.htm

Overview of bloc positions with regards to ISIS:

- http://www.cnn.com/2015/11/20/world/war-on-isis-whos-doing-what/index.html

Case studies:

- Overview of Sinjar Massacre: http://www.cnn.com/2014/08/10/world/meast/iraq-isis-sinjar/index.html
- Overview of 2010 Palestinian militancy campaign: http://www.irishtimes.com/news/islamist-groups-attempt-to-derail-middle-east-talks-1.646680

SOURCES

TOPIC 1

Bloc Positions

https://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition

http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism

https://www.wired.com/2014/11/what-is-a-zero-day/

https://www.wired.com/2015/04/dods-new-transparent-policy-cybersecurity-still-opaque/

https://www.gov.uk/government/policies/cyber-security

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

http://www.cpni.gov.uk/advice/cyber/

https://cybersecuritychallenge.org.uk/

http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/

http://www.ecs-org.eu/

TOPIC 2

Topic Intro

http://www.nato.int/cps/en/natohq/topics_77646.htm

http://www.globalresearch.ca/whats-the-big-difference-between-natos-moderates-and-extremists-in-syria/5527095

http://www.jpost.com/Opinion/NATO-vs-ISIS-374702

http://www.voanews.com/content/greater-nato-unity-seen-against-islamic-state-russia-challenges/3337865.html

https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant

http://news.antiwar.com/2016/05/18/us-envoy-nato-doesnt-have-to-join-isis-war-so-long-as-it-participates/

http://www.cnn.com/2015/11/20/world/war-on-isis-whos-doing-what/index.html

http://blogs.timesofisrael.com/has-the-war-against-isis-forced-the-us-and-russia-to-return-to-the-cold-war/

History

http://www.nato.int/cps/en/natohq/topics_77646.htm

http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/modern.html

https://www.rt.com/uk/224159-terrorism-worse-cold-war/

http://thediplomat.com/2014/07/isis-a-threat-well-beyond-the-middle-east/

https://web.archive.org/web/20110927084019/http://www.g8.fr/evian/english/navigation/g8_documents/archives_from_previous_summits/kananaskis_summit_-_2002/g8_counter-terrorism_cooperation_since_september_11th_backgrounder.html

Bloc Positions

www.businessinsider.com/belgian-fighters-in-iraqsyria--isis-2014-9

www.cnn.com/2015/01/15/world/belgium-anti-terror-operation/index.html

http://newsbout.com/Daily+Mail/tag/Bulgaria+ISIS+Wants+Dinko+Valev

http://www.balkaninsight.com/en/article/the-roma-and-the-radicals-bulgaria-s-alleged-isis-support-base-01-10-2016-1

http://www.czech.cz/en/News/Czech-Republic-ready-to-do-more-in-war-against-ISIS

www.baltictimes.com/news/articles/35768

www.cnn.com/2015/11/15/middleeast/france-announces-raqqa-airstrikes

http://www.nytimes.com/2014/09/13/world/europe/germany-bans-support-of-isis.html

http://www.independent.co.uk/news/world/europe/greece-threatens-to-unleash-wave-of-migrants-on-the-rest-of-europe-including-isis-jihadists-10097432.html

http://www.iraqinews.com/iraq-war/hungary-send-troops-iraq-join-fight-isis/

www.nytimes.com/2014/11/22/world/middleeast/isis-taunts-united-states-and-britain-in-new-video.html?_r=0

www.cnn.com/2014/10/23/world/canada-isis-role/index.html

www.history.com/topics/9-11-attacks

https://www.foreignaffairs.com/articles/iraq/2007-01-01/united-states-iraq-and-war-terror

www.abcnews.go.com/WN/fullpage/isis-trail-terror-isis-threat-us-25053190

www.cnn.com/2014/08/28/world/meast/us-options-syria/index.html