CONTENTS

Letter from the Chair ................................................................. 3

Topic A: ................................................................. [4]
  Introduction ................................................................. [4]
  History of the Topic ........................................................ [5]
  Current Status ............................................................ [8]
  Country Policy ............................................................ [13]
  Keywords ................................................................. [15]
  Questions for Consideration ........................................... [17]

Topic B: ................................................................. [20]
  Introduction ................................................................. [20]
  History of the Topic ........................................................ [21]
  Current Status ............................................................ [25]
  Country Policy ............................................................ [31]
  Keywords ................................................................. [33]
  Questions for Consideration ........................................... [34]
LETTER FROM THE CHAIR

Dear Delegates,

Glad to have you guys here at PMUNC! My name is Maia Hamin, I’m a sophomore student hailing from the great state of Massachusetts. At Princeton, I’m planning to declare a major in Computer Science, and I’m interested in potentially pursuing a certificate --- a minor, in case you don’t study Princeton nomenclature in your spare time --- in Robotics and Intelligent Systems, or maybe Technology and Society. This will be my second year helping staff PMUNC; I was a director in SPECPOL last year, where we discussed the Kashmir conflict and land rights in the Arctic Circle. I also competed as a delegate for several years in high school, in both general assemblies and specialized committees. At Princeton, when I’m not slaving away over your background guides, I’m writing and editing for our on-campus humor magazine, Tiger Mag, and playing on the women’s ultimate frisbee team.

Our first topic is one near and dear to both my academic interests and my paranoid heart: global cybersecurity infrastructure and cyberespionage countermeasures. As more and more of our social, commercial, and political activities are conducted online, both citizens and governments become increasingly vulnerable to security breaches with far-reaching consequences. Critical financial, communication, infrastructure, weapons, and voting systems in every nation are internet-connected and therefore vulnerable. Ought NATO to protect its member states from acts of cyberwarfare? Should it take an active role in mandating cybersecurity measures to prevent catastrophic failures? Are there limits to the types of subversive digital activity that its members can be permitted to undertake? All of these and more are pressing questions, matters in which most inter- and national bodies have lagged behind the blistering pace of technological advancement.

Our second topic is more traditional but no less pressing: the rise of authoritarianism in the government of Turkish president Recep Tayyip Erdogan. Reports of corruption, human rights violations, and suppression of the press, followed in 2016 by an unsuccessful coup attempt and resultant state of emergency declaration (which is still in effect), culminated in the highly-disputed April 2017 Constitutional Referendum, which endowed the Turkish President with far-reaching executive powers and restructured the judiciary. Still officially in the process of negotiations to join the European Union, Turkey’s longstanding Western alliances are on increasingly thin ice due to concerns about these authoritarian moves, even as Turkey remains a powerful influence in the Syrian conflict and the region at large. How should NATO respond to concerns about potential dismantlement of democratic processes by a member state? What strategic risks does NATO run in criticizing or punishing the Erdogan regime? A multilateral consensus is needed to guide NATO policy in this matter and to avert the destructive consequences of a political misstep in the already-fraught region.

Both of these issues are hugely complex, and both lack clear and universally-popular solutions --- precisely what makes for good debate. Delegates from every country can (and, I’m sure, will!) formulate realistic and detailed policy proposals in line with their countries interests. For both topics, being well-researched about both the topic at hand and your country will be of the utmost importance. Please feel free to reach out about either, since I could talk for ages about both!

So excited to meet you all,

Maia Hamin
TOPIC A: International Cybersecurity

Introduction

The Digital Revolution has, like its Industrial counterpart, radically changed every facet of modern human life. The blinding speed of technological advancement has brought countless improvements in sectors from healthcare to finance and industrial engineering to social networking, through the ability to rapidly send, receive, create and interpret massive amounts of data. The interconnected nature of the internet has also, however, created a whole host of new vulnerabilities. More and more, we are seeing state and non-state actors begin to exploit these vulnerabilities to advance their interests on the global stage.

Specific digital threats to entire nations come in many forms, and from many sources. Attackers might seek classified information to learn the identities of intelligence operatives, anticipate troop movements in a conflict, or blackmail prominent leaders. Hacking could compromise the results of electronic voting, or allow an adversary to steal valuable technological secrets. Cyberterrorists could create deliberate failures in internet-reliant infrastructure, like nuclear plants, power stations, or dams. Some threats to safety and liberty may come from governments themselves: leaks have revealed that many global governments are conducting extensive and largely undisclosed surveillance on their citizens and citizens of many other countries.

The essential problem of cybersecurity is that the internet has no governing body, no central authority. By whom cybersecurity measures should be implemented is as much a question as is what measures might be necessary. Should private corporations be asked to step up and shoulder the burden? Should national governments ask this of them, or should they only look after the security of their own systems? There are no easy answers to these questions, even for experts, but the mounting dangers posed by cyber threats demand, at the least, our best attempt to create a safer digital world.
History of the topic

Any attempt at technological legislation must be premised not only on an understanding of international law and precedent, but upon a basic understanding of the technology at hand; legislators must know what is and is not possible to mandate before they issue sweeping edicts. The internet is complicated and nebulous in its structure, but basic facts about its design will help us understand how it can be regulated.

First, a bit of history. The Internet began in the 1960’s in the US Department of Defense’s Advanced Research Projects Agency as an attempt to connect geographically-distant computers. This first incarnation, called ARPANET, was primarily used to connect research computers until the 1990s, when commercialization turned it into something closer to the internet we know and love today.¹ The internet today is an interconnected network of computer networks (a meta-network of sorts) that can be used to transmit massive amount of data between distant locations. Data from an individual computer is broken into ‘packets’ of binary bits and then routed through a hierarchy of connected nodes until it reaches its destination. The path that it takes is specified by so-called ‘routing protocol’, where each ‘router’ that a package flows through will send it to the next point in the fastest path to its destination. On its way from source to destination, a packet may travel through servers across multiple countries or even continents; the optimal routing path is also determined in real time, making it difficult to retrace the exact path that a packet may have taken.²

It’s important to understand that the Internet has no central governing body: individual networks may have policies for traffic that flows through their servers, but there is no way to enforce standardized content or security procedures across every network that traffic flows through. Routing and communication protocols are specified by the Internet protocol suite (TCP/IP), which

² Kernighan, Brian W.
is maintained by the Internet Engineering Task Force (IETF), a non-profit organization that sets
standards so that these autonomous networks can connect and communicate. Domain names and IP
addresses, the unique identifiers by which websites are located and indexed, are allotted by the
Internet Corporation for Assigned Names and Numbers (ICANN), and often distributed by
intracontinental bodies, such as the American Registry for Internet Numbers (ARIN) for North
America and the Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe,
the Middle East, and Central Asia.³ Beyond these bodies, which merely facilitate communication, the
internet’s structure is one of a complex and organic web with no centralized oversight.

International precedent for regulation of the internet is sparse. The explosion of the Internet
into every corner of life has been relatively recent, in the scale of international political time. Even
sparser is the relevant legislation on the topic of malicious cyber attacks and national cyber security.
Much of current international debate revolves around the extension of conventional treaties to the
digital domain. The UN has substantial literature on the laws of war, including, notably, the Geneva
Conventions. These documents mainly address conventional concerns such as the humane
treatment of prisoners, but Article 50 of Protocol I specifies that noncombatants should not be
targeted, and Chapter III of Protocol I lays out rules for the targeting of civilian objects and
structures.⁴ Do these rules apply to digital personas or digital infrastructure? NATO’s charter, as laid
out above, contains a collective defense clause triggered by an attack on a member country. Would a
cyber attack qualify for this clause? Of what magnitude? Many countries have made moves towards
recognizing cyber attacks as *casus belli* for a declaration of war, just as conventional attacks would be.⁵

³ Kernighan, Brian W.
⁴ International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of
War (Fourth Geneva Convention)*, 12 August 1949
Whether this means that a cyber attack of sufficient magnitude could merit a boots-on-the-ground response remains to be seen --- or decided.

International response to cybercrime has some more legislative precedent, albeit not by much. The 2001 Budapest Convention on Cybercrime is the only major legislative work on cybercrime in international law. It was drawn up by the Council of Europe, and has since been ratified by 52 states. The Convention’s main objective was to lay out a framework for member states to implement new cybercrime laws, and to facilitate international cooperation in the prosecution of cybercriminals. Its suggestions for member countries laid out several categories of digital crimes, such as illegal access, digital copyright infringement, digital fraud, and offences related to the distribution of child pornography. Its Additional Protocol (which not all signatories have ratified) called for the criminalization of online publication of racist and xenophobic material. This legislation represents one of the first significant attempts to lay out international standards for the digital realm.

Regional bodies, such as NATO, and specific countries have adopted cybersecurity-specific legislation, outlined further in the next section, which provides a useful framework for building further consensus. Cybersecurity strategies and efficacy differ wildly between countries, and thus each country’s goals in a multilateral discussion of cybersecurity will vary.

---


7 "Details Of Treaty No. 185".
Current situation

Cybersecurity is information protection developed as a response to forms of cyber crime or warfare. Cyber warfare, broadly, encompasses two parts. The first is cyber espionage: like traditional espionage, cyber espionage is often unilaterally illegal, and is, like its conventional counterpart, typically assumed to be carried out by most national powers against rivals. Cyber espionage typically involves accessing secure data or snooping on secure communications of a foreign power or foreign citizens. This may take place through ‘packet snooping’ at routers, through hacking of communications databases, phishing attempts, or, as in the United States, through the (mandatory) cooperation of commercial partners. The classified documents leaked by former NSA contractor Edward Snowden revealed the existence of the so-called PRISM program in the United States, in which the National Security Agency (NSA) obtained the communications and usage data of users of interest from at least nine major tech companies --- including Google. Though intercepting foreign communications is seen as a legitimate form of espionage, many countries have laws against monitoring the communications and online activities of their own citizens (though the exceptions to this rule are rather extensive in many countries). Some countries engage in intelligence sharing, allowing them to circumvent domestic regulations and accrue additional data on their own citizens as well as foreigners. The ‘Five Eyes’ organization, comprised of the US, UK, Canada, Australia, and New Zealand, is one of the most well-known intelligence alliances in the world (though there are Six-, Nine-, and Fourteen Eyes groups that generally involve the Five plus additional, often European, members). Collectively, they have amassed staggering records of communications of billions of people around the world.

---

Like traditional espionage, cyber espionage has led to international incident. The Snowden leaks revealed that the US had been effectively wiretapping Angela Merkel, the leader of US-allied Germany\textsuperscript{9}, triggering international condemnation. Often, the connections between attackers and governments are harder to prove: US officials have alleged that state-sponsored Chinese hackers were behind ‘Titan Rain’, the set of attacks between 2003 and 2006 which targeted US defense companies, but have yet to provide definitive evidence of Chinese government involvement.\textsuperscript{10} The US’s claim, and China’s denial, have caused serious friction between the two world powers, and has led other leaders to worry that their systems might have been subject to a similar hacking scheme that simply went undetected.\textsuperscript{11} To make things even more difficult, espionage is not the only motivation for theft of secrets. Titan Rain may have been an attempt to steal intellectual secrets and patent information from US companies, which would make it a form of prosecutable cyber crime rather than an international incident.

The US government may fear, however, that Titan Rain was an attempted example of the second, and more malicious, form of cyber warfare: active attack or sabotage through digital channels. The most significant example of a cyber attack on an entire country was a 2007 Distributed Denial of Service (DDoS) attack in Estonia. A DDoS attack occurs when hackers use one or more computers --- often a botnet, a large network of computers taken over remotely to execute a specific task --- to inundate a website with requests until its servers are overrun and it ceases to function. In this case, the overwhelming of key servers and sites in Estonia’s digital infrastructure temporarily disabled most of the country’s online systems, including health care, online banking, mobile data, and government services. This attack came in the middle of Estonia’s

\textsuperscript{9} Angwin, Julia, and Jeff Larson.
\textsuperscript{11} Thornburg, Nathan.
dispute with Russia over the Bronze Soldier of Tallinn, which Estonia wished to relocate. Though
the Estonian government has long alleged that Russia was behind the DDoS attacks, no definitive
proof has emerged that it was a state-sponsored act of aggression.\textsuperscript{12}

Definitively proving a foreign government’s involvement in a cyber attack is difficult and
often a source of controversy. The malicious worm Stuxnet that targeted industrial computer
systems and hampered Iran’s nuclear program seems to have been a US-Israeli-constructed
cyberweapon, but neither government has openly admitted responsibility.\textsuperscript{13} Hacking or attempted
hacking of election-related emails in the United States, Denmark, and France has escalated tensions
with Russia, whence the attacks may have originated, though the Kremlin has denied involvement.
The “Red October” cyber attack exploited vulnerabilities in Microsoft programs for years to steal
information from governments, embassies, militaries, and research groups in Eastern Europe for the
benefit of persons still unknown.\textsuperscript{14} Further complicating the issue is the fact that attacks can also be
carried out by non-governmental organizations: lone hackers who enjoy creating confusion or
gaining recognition through disruption of government sites; organized cybercrime syndicates
looking for financial gain through hacking; terrorists who wish to harm the government by harming
its people; or ‘hacktivists’ who attack to create political change through information exposure or
punitive disruption. The lines between these categories are not clear, and the anonymity offered by
the digital world can create further obfuscation. For many of the dozens of attacks that occur every
year, the exact perpetrators remain unknown and unpunished, and the involvement of foreign
governments in these acts of cyber aggression remains enigmatic and difficult to prove.

CCDCOE.
\textsuperscript{13} “The History Of Cyber Attacks - A Timeline”.
\textsuperscript{14} “The History Of Cyber Attacks - A Timeline”. 2017. NATO Review.
Many countries are actively working to build their cyber security and cyber warfare capabilities. National bodies like the UK’s National Cyber Security Centre (NCSC) and regional partnerships like the European Union Agency for Network and Information Security (ENISA) have been formed in recent years to improve national government’s security protocols. There are several types of security which national actors are working to refine and implement. Firewalls, systems which monitor traffic between an internal and external network, are the most common way that large organizations secure their data. Their firewalls filter out malicious packets from the external network, the Internet, that seek to access the secure networks and data accessible to those within the organization. Malware protection is a type of proactive security which seeks to prevent the installation of malicious software onto computers, through educating users about safe use practices, and through thorough scanning of files and applications for dangerous elements. Many systems that handle sensitive or desirable data also implement programs which detect attempted interference in multiple forms, so that attacks can be mitigated or attackers found before their programs successfully exploit a system vulnerability.

Information security is also provided by cryptography, which, essentially, scrambles a message as it is transmitted through a medium (like the Internet) or stored in a database, in such a way that it can be unscrambled when it reaches its destination. Thus, if anyone is listening in the middle, the message is useless gibberish. The most popular form of encryption in use today is public key cryptography (the mechanics of which are a little beyond the scope of this background guide). More and more websites are turning towards using encrypted protocols to protect user data from malicious interference. Some messaging services use ‘end-to-end’ encryption (E2EE), which ensures

---

16 Common Cyber Attacks.
that a message can only be read by the intended recipient, because it is encrypted from the start of its journey until it reaches its destination.\textsuperscript{17} Many governments disapprove of or disallow the use of messenger applications that use EE2E, because it prevents them from being able to monitor the conversations --- Whatsapp is blocked in twelve countries currently.\textsuperscript{18} ‘Back doors’, workarounds that allow companies to access secure user information, sometimes give companies a loophole that keeps them in good graces with a disapproving government. The Snowden revelations included evidence that Microsoft maintained such a ‘back door’ in Skype that provided US officials access to subpoenaed messages, even though the service is officially E2EE.\textsuperscript{19} The issue is nuanced: for every free-speech activist using Whatsapp to hide details of a protest from an oppressive regime, there is a human trafficker using Whatsapp to avoid detection by the authorities. The debate over what information should be encrypted is ongoing and complex.

NATO itself has recognized the need for urgent action on the digital frontier. In the Wales summit of 2014, NATO allies adopted a resolution that, “establishes that cyber defence is part of the Alliance’s core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO’s cooperation with industry.”\textsuperscript{20} NATO’s existing cybersecurity infrastructure includes the NATO Computer Incident Response Capability (NCIRC), which provides defense support to NATO-owned networks. NATO also promotes collective cyber defense through its Smart Defense program, recently expanded to the digital sphere, which encourages sharing of security resources between member countries. Smart Defense cyber projects include the Malware Information Sharing Platform (MISP), the Smart Defence Multinational Cyber Defence Capability

\textsuperscript{17} Kernighan, Brian W.
\textsuperscript{19} Angwin, Julia, and Jeff Larson.
Development (MNCD2) project, and the Multinational Cyber Defence Education and Training (MNCDET) project. NATO also invites member countries to participate in non-mandatory training exercises at its annual Cyber Coalition Exercise. Training and research also occurs at the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia; the NATO Communications and Information Systems School (NCISS) in Latina, Italy; and the NATO School in Oberammergau, Germany.

Understanding the existing solutions of NATO allows us to conceive of ways to expand, alter, or curtail the current cybersecurity agenda of the Alliance. Unfortunately for us, policy makers cannot create the actual security measures that stop hackers. What we can control, as international policy makers, are the elements of security strategy that happen on the global scale: the allocation of resources to cyber security as a part of the national defense budget; our country’s foreign policy response to cyber warfare incidents; guidelines for appropriate investigation and sentencing of those who violate digital law; rules about encryption and freedom of expression on digital platforms. These defense-oriented digital policy questions are deeply important to NATO’s mission as a collective defense organization, and indeed for the future of the internet as a tool for progress --- or chaos.

**Country policy**

**US, UK, Canada:** Members of the ‘Five Eyes’ program and thus all privy to more sensitive intelligence information than many other countries --- and likely interested in preserving this special status. All have a vested interest in preventing digital attacks, especially those aimed at intellectual property --- the US is the nation most affected by far by cyber espionage and intellectual property

---

21 “Cyber Defence”.
The UK recently suffered from ransomware attacks and has pledged new focus on cybersecurity. The three represent technological leaders who conduct extensive surveillance on their own citizens and allies. The US NSA and its other intelligence agencies are known for holding onto dangerous zero-day exploits and backdoors, which they may be very reluctant to share, even amongst the bloc.

**Germany, France, Spain:** Non-Five-Eyes countries with relatively strong cyber security who tend to be targets of cyber espionage. France was the victim of attempted election email hacking, potentially by Russia. Germany learned from the Snowden revelations that the US was spying on Chancellor Angela Merkel. All three are generally close allies of Five Eyes Members, so they may push for inclusion or increased intelligence sharing and transparency.

**Poland, Estonia:** Two up-and-coming countries investing heavily in improving their cybersecurity systems. Poland is interested in becoming an economic leader in cybersecurity through education initiatives. Estonia has invested in extensive cybersecurity measures since the 2007 attacks, and is likely to worry most about another Russian cyberattack.

**Latvia, Lithuania, Romania, Bulgaria:** Geographically close to Russia and thus most worried about Russian cyber capabilities and conflict with Russia. Tend to have weaker cybersecurity measures than other NATO countries.

---


23 Angwin, Julia, and Jeff Larson.

24 Goud, Naveen.


26 Tikk, Eneken, Kadri Kaska, and Liis Vihul.

27 Goud, Naveen.
Norway, Iceland, Denmark, Belgium, Netherlands: Countries with highly secure cyber defense measures and strong economies. These countries don’t need as much international assistance with their programs, though they have plenty of expertise to offer.

Greece, Italy, Portugal: Countries without strong cybersecurity infrastructure that lack excessive money to spend on building new. They stand to benefit from collective defense agreements that don’t demand too much from their own resources.

Hungary, Albania, Croatia, Slovakia, Slovenia, Czech Republic, Luxembourg: Countries heavily dependent on collaborative frameworks from NATO or ENISA for cyber security. Likely to push for further help developing guidelines and training specialists to shore up defense systems.

Turkey: Active focus on recruiting new specialists and improving cyber defenses, but also in the middle of an authoritarian seizure of power. The NATO country with the poorest record of internet freedom.

Keywords

**Botnet:** a network of innocent internet-connected devices which have been taken over by a remote hacker and can be used to perform coordinated attacks, like DDoS attacks, that require a lot of computing power

**Casus Belli:** a justification for a declaration of war

**Cryptography:** a method of secure communication or data exchange that scrambles data in transit to protect it from ‘man in the middle’ attacks and unscrambles it at its destination so it can be read

---

28 Goud, Naveen.
31 Kelly, Sanja.
Cyber- : a prefix describing a form of the stem word that happens online or on a computer, e.g. cybercrime, cybersecurity, cyberwarfare

DDoS Attack: a Dedicated Denial of Service Attack, happens when a malicious party uses multiple machines to send repeated requests to a single website or server, giving it more traffic than it can handle and thus preventing other users from accessing it for some period of time.

Firewall: a popular form of security, a program that connects two networks and filters incoming traffic from one (often the internet) to prevent harm to the other

Intellectual Property: patents, copyrights, trade secrets, and other forms of information protected by law from infringement. Unauthorized access to intellectual property allows competition to potentially undercut existing manufacturers by using their processes illegally.

Internet Engineering Task Force (IETF): a non-profit organization that sets non-binding technological and linguistic standards that enable the independent networks that comprise the Internet to exchange information, thus facilitating the function of the Internet network as a whole

Malware: malicious software, installed on someone’s computer. E.g. ransomware, which locks a computer and holds its contents hostage for payment, or used to make a computer a ‘bot’ that performs some malicious action, like a DDoS attack, at the hacker’s command

Zero-day vulnerability: a vulnerability is an error or a weakness in a system or software that could potentially be exploited by hackers. A zero-day vulnerability is one not already known to the system manufacturers: a vulnerability that they will have “zero days” to patch or fix before it is exploited. Some intelligence agencies, notably the NSA, hold onto known zero-day vulnerabilities that allow them to hack commercial software, leaving these vulnerabilities intact for others to potentially use.
Questions:

- How much of a threat are cyber attacks, compared to conventional military attacks? Does NATO need to allocate more resources to cybersecurity, or fewer?
- Do cyber attacks trigger the collective defense clause of NATO’s charter? If so, are there criteria regarding severity and response type? Is this response limited to a cyber response, or could it be physical military action?
- Should NATO member countries be held to a standard of cyber security? If so, how should NATO outline the necessary standards?
- Should NATO form any additional bodies to handle cyber threats? How would these bodies operate?
- What are the limits on acceptable forms of cyber espionage between NATO allies? On non-member countries?
- Should NATO allies share intelligence? Security protocols? Information about vulnerabilities?
- What role do private corporations play in the digital landscape of the future? Should NATO member countries standardize mandatory operating procedures for technological companies operating within their borders?
- What does the future of international organizations look like in the digital age? How will rapidly accelerating technological change and the democratization and globalization of the internet change the international political sphere? Does NATO need to change its mission or its structure to stay relevant and impactful in this changed landscape?

Additional Readings:

- “Introduction to the Internet and WWW”, Peter Gao
  - [http://www.engr.sjsu.edu/gaojerry/course/cmpe296u/slides/introduction.pdf](http://www.engr.sjsu.edu/gaojerry/course/cmpe296u/slides/introduction.pdf)
• “Introduction to Cyber Security”, online course:
  o https://cybersecuritybase.github.io/introduction/
• “Cybersecurity and International Law” (PowerPoint presentation):
  o http://www.hoover.org/sites/default/files/waxman_stanford_cyber_presentation.pdf
• “Cyber defence”, NATO:
  o http://www.nato.int/cps/en/natohq/topics_78170.htm
• “Cybersecurity and the need for international governance”, National Law Review:
• Cyber Defense Review (magazine published by US military):
  o http://cyberdefensereview.army.mil/
• The Internet Society (entire webpage with useful sections):
  o https://www.internetsociety.org/
• “D is for Digital”, by Brian Kernighan (an excellent book, for those interested in learning more about the digital world)

References


TOPIC B: Authoritarianism in Turkey

Introduction

NATO has historically been, in its own view at least, a champion of democracy and human rights across the globe. To join, member states must demonstrate a commitment to democracy, rule of law, and the protection of human rights. NATO has, in its past, intervened militarily and diplomatically when they’ve felt that a country’s territorial integrity or its people were gravely threatened. The recent events in Turkey, then, which include ideological purges of dissidents and minorities and a consolidation of dangerous executive power, pose a pressing and existential question to the member states of NATO. Erdogan’s words and actions suggest that democracy and checks on authoritarianism are ever more imperiled in Turkey, thus putting NATO in the difficult position of having to decide how to handle its deepest convictions when they potentially conflict with its strategic goals.

The advantages that Turkey brings to the Alliance are not to be discounted, as the second-largest military in a location of great strategic importance. It has allies within the bloc who stand to gain from its continued favor and from economic integration with international bodies like the European Union. However, Turkey’s increasing overtures towards Russia and conflicts with the United States over rebel groups in the Syrian Civil War may be signs that an unavoidable conflict is shaping up within the ranks of NATO. The decisions made about how to handle member state’s domestic problems within the cooperative international body that is NATO may profoundly shape the strategies and goals of the institution for decades to come. In this committee, Turkey is intended more as an example of as existential question for NATO than as a single circumstance in need of resolution: it is more urgent that NATO resolve the question of standards and potential punishments for member countries than that it is you, as delegates, simply solve this crisis.
International law attempts to create frameworks for ongoing conflict resolution, and it would behoove delegates greatly to maintain this long-term focus as we discuss the issues at hand.

**History of the topic**

The modern-day Republic of Turkey, with its historical roots in the Seljuk and Ottoman Empires, began following the Turkish War of Independence (1919 - 1922), which was caused by a Turkish nationalist movement against Allied occupation of previously-Ottoman territory in the wake of WWI. The 1922 abolition of the 600-year-old Ottoman sultanate and the 1923 signing of the Lausanne Treaty, granting Turkey sovereignty within its own borders, allowed military commander Mustafa Kemal (later given the honorary surname Ataturk) to become the first President of the nascent Republic of Turkey in 1923. Ataturk’s ideology came to be known as Kemalism and provided the founding principles which govern have historically governed the Republic of Turkey: democracy, nationalism, secularism, interventionism for domestic social and economic gain, and a general commitment to Westernization. Broadly speaking, Kemalism has been popular in Turkey, with its increased focus on education and quality of life improvements for the citizens and its moves away from the authoritarianism of the Ottoman Sultanate. The Turkish Armed Forces (TSK) and the judiciary have historically regarded themselves as protectors of Kemalism, and have forced several regime changes when they felt that secularism was under threat: two military coups d’etat, in 1960 and 1980, and two military injunctions, in 1971 and 1997.

Internationally, Turkey has been roughly aligned with the West since Ataturk’s presidency. Turkey remained officially neutral during WWII, but declared war on Germany and Japan in the

---


33 Kili, Suna.
war’s final months, allowing them to join the newly formed United Nations after its end. During the Cold War, Soviet pressure for Turkey to accept the installation of military bases in the Turkish Straits led Turkey to align itself with the US and its newly-issued Truman Doctrine.\textsuperscript{34} Turkey was therefore an early member of NATO, joining the Alliance in 1952 during the early years of the Cold War. Since 1980, it has focused increasingly on economic liberalization and international cooperation, joining the European Economic Community in 1987 and beginning the process for becoming a member of the EU in 2005. Turkey’s role in NATO has always been bolstered by its strategic location in several conflicts. During the Cold War, Turkey was a convenient base of operations for operations targeting nearby Russia. Then, and even after the dissolution of the Soviet Union, Turkey’s proximity to the Middle East has been an important strategic asset to NATO in its attempt to stabilize the region and exert its influence. During the Cold War, Turkey helped NATO to prevent Russian meddling in the Middle East as a signatory to the 1955 Bagdad Pact. This treaty formed the Central Treaty Organization (CENTO), a collective-defense agreement between Iran, Iraq, Pakistan, Turkey, and the UK (with the US joining the command in 1958) that was modelled after NATO.\textsuperscript{35} Designed to repel Soviet incursion across its southwestern border, CENTO was ineffective, partially due to its lack of centralized military command and partially because of regional instability. The alliance largely declined to intervene in regional conflicts like the first Arab-Israeli War and two different Indo-Pakistani wars\textsuperscript{36} The alliance was incredibly strained by the departure of Iraq following a coup by the pro-Soviet Iraqi nationalist Abd al-Karim Qasim in 1958, and by Turkey’s 1974 invasion of Cyprus. It formally dissolved following the 1979 Iranian Revolution,

\textsuperscript{36} “The Baghdad Pact (1955) and the Central Treaty Organization (CENTO).”
when the newly-formed Islamic Republic government, led by Ayatollah Khomeini, withdrew from the pact.

After the fall of the Iranian monarchy and the dissolution of CENTO, Turkey’s importance to NATO as a “functional ally” --- a country that possesses vital military or diplomatic advantages without being a key player in the alliance’s mission and strategy --- grew. Its proximity to Iraq was useful as a quick-response operations base to the allied coalition --- which included many NATO members --- that fought in the 1991 Gulf War. Turkey’s internal foreign policy strategies began to shift, as it looked to take a more active role in Middle Eastern affairs and become more of a strategic leader within NATO. It has increasingly looked to NATO as an important asset to force multilateralism in the region. Turkey’s government was an outspoken opponent of the 2011 French-led airstrikes in Libya, advocating instead for a NATO takeover of the UN-sanctioned military operation against the Gaddafi government, which would have given Turkey a strategic voice in the conflict and possibly veto power over the airstrikes. It has invoked Article 4 of NATO’s charter, which demands consultation among the Alliance in response to a military threat, four times: once in 2003 in response to the mounting Iraq War; twice in 2012 over the Syrian Civil War, after an unarmed Turkish F-4 reconnaissance jet was downed and after a mortar was fired across the Syrian-Turkish border; and once in 2015 to address threats to its territory by the Islamic State. NATO itself is reliant on Turkey, which maintains the second-largest active military within the coalition and is of vital importance in the refugee crisis roiling Europe: in 2017, for the third year in a row, Turkey was

37 Aybat, Gulnur.
38 Aybat, Gulner.
the country that accepted the highest number of refugees in the world. 3 million displaced Syrians now live, predominantly in refugee camps, within Turkey’s borders. 40

Never in NATO history has a country been removed from the Alliance. The 1995 Study on NATO Enlargement laid out NATO’s ‘open door’ policy, in which any country that wishes to join, can demonstrate that they will further the goals of Western security, and meets standards of freedom and democracy is permitted to join the alliance. Specifically, the document recommends that applicant countries should have:

- “a functioning democratic political system based on a market economy;
- the fair treatment of minority populations;
- a commitment to the peaceful resolution of conflicts;
- the ability and willingness to make a military contribution to NATO operations; and
- a commitment to democratic civil-military relations and institutional structures.” 41

NATO does not have a well-developed punitive mechanism, since it is an organization premised on sovereignty and voluntary cooperation. Many member countries do not meet organizational requirements such as the spending mandate --- only five member countries currently meet the required threshold of defense spending measuring at least 2% of their GDP42 --- and NATO has not levied sanctions or restrictions on these non-compliers. In past cases where NATO member countries have shown troubling signs of deteriorating democratic processes, no formal NATO response was ever standardized. In the cases of both a 1967 military coup in Greece and the 1960 and 1971 coups in Turkey, the reaction from Alliance countries varied. Some NATO allies, like Norway, Denmark, and the Netherlands, pushed for a strong response from NATO in the form of possible investigations, arms embargos, or even expulsions. Other, and larger, countries like the

---


United States and the United Kingdom, wanted to prioritize Alliance stability at the height of the Cold War by protecting Greek and Turkish membership, even at the expense of keeping silent about their undemocratic regime changes. The larger countries won out, and, to date, no member country has ever been expelled from NATO. The question of how to resolve such cases in the future, cases such as the situation in modern-day Turkey, has yet to be answered.

Current Situation

Turkey’s relationship with NATO has become increasingly fraught in the wake of changes in its domestic and international policies. The current president of Turkey is Recep Tayyip Erdoğan, who was the first president elected by a direct popular vote. He previously served as Prime Minister (a role now occupied by Binali Yıldırım) from 2003 to 2014, and before that was the Mayor of Istanbul. He established the moderate conservative Justice and Development Party (AKP), and was praised in the early years of his leadership for steering the country towards recovery after a 2001 financial crisis, pursuing a multilateralist and neoliberal foreign policy by entering talks to join the EU and increasing trade and infrastructure investment, and beginning talks in 2012 with the Kurdish Worker’s Party (PKK) to end the insurgency that began in 1978 (though the ceasefire fell apart in 2015 and hostilities recommenced).^{43}

Even in the early years, shadows of scandal hung over the AKP’s rule in Turkey. The “Ergenekon” trials were a series of prosecutions of alleged members of the ‘Ergenekon’ society, a secret ultranationalist Kemalist group that prosecutors alleged was behind nearly every act of political violence and militancy in recent Turkish history. Beginning in 2008, security courts began to try some of the nearly 500 people accused of membership in the society. Since the beginning,

---

journalists and dissidents have alleged that many of the accused were merely opponents of the ruling AKP party, and in 2015 forensic experts found that many of the incriminating documents were fakes. \(^\text{44}\) Other journalists have alleged that the Ergenekon prosecutions were related to the Gülenist movement, a conservative Islamist movement led by Turkish preacher Fethullah Gülen that was, in 2008, a close ally of the AKP party. The two parties had formed an alliance in the early 2000s against the secularist establishment, which allowed AKP to win elections and form a majority government, and gave Gülenist politicians avenues to gain more political power in the traditionally-secular Turkish government. A journalist, Ahmet Şık, who was writing a book on Gülenist infiltration of the country’s secret police, was arrested for involvement in the Ergenekon affair, even though he himself was investigating the existence of a secret society. His drafts were confiscated and possession of the book banned, causing many to suspect that the Gülenist movement was exerting heavy political influence under the AKP regime of the 2000s. \(^\text{45}\)

The end of the AKP-Gülenist alliance came in 2013, when Erdogan was still Prime Minister, after a 2013 corruption scandal involving bribery, money laundering, and “gas-for-gold” trading with Iran that implicated 52 people connected with Erdogan’s AKP party, including government officials and their family members. \(^\text{46}\) Before promised evidence that might have implicated Erdogan’s sons emerged, his government dismissed hundreds of prosecutors, police officers, and other judicial officials who were involved with the ongoing investigation, alleging that the charges were an international conspiracy perpetrated by the followers of Fethullah Gülen, whose teachings they denounced as terroristic. \(^\text{47}\) The scandal prompted the resignation of dozens of AKP politicians

\[^{45}\text{“Timeline: Turkey’s Ergenekon trial.”}\]
\[^{47}\text{Coskun, Orhan, and Ece Toksabay.}\]
implicated by the preliminary reports, forcing the AKP to reshuffle its cabinet, and setting a precedent of AKP persecution of perceived Gülenists. This bitter rivalry may have been involved in the infamous coup attempt that precipitated the downward spiral of Turkey’s democracy.

The coup began on July 15, 2016, around 11 pm, when several high-ranking government officials were seized by armed rebels who attempted to force them to sign documents ceding control of the government. The insurgents controlled several fighter planes, tanks, and helicopters, and used these to bomb police headquarters outside of Ankara, resulting in dozens of casualties. Just after midnight, the rebel group successfully took over a broadcast station, where they forced a news anchor to read a statement that described how the current administration had eroded the secular rule of law in Turkey, stated that, therefore, the country was now under the control of the “Peace at Home Council”, laid out the organization’s goals to preserve human rights and the rule of law, and then declared martial law.  

President Erdogan was on vacation in southern Turkey at the time of the coup. His messages to the people started around 12:30, promising them that he was still in control of the government and urging them to take to the streets in defiance of the order of martial law. His plane returned to Ankara just before 3 am. Loyalist forces within the Turkish Armed Forces (TSK) and civilians stormed the broadcasting headquarters and the airport and retook them from the insurgents. At various points in the night, gunfire and bombs went off at the Parliament building and the hotel where Erdogan had stayed for a few hours. Several surviving rebels took a helicopter to Greece, where they petitioned for asylum (nearly all were denied). Civilians took to the streets in massive numbers to protest the coup, causing confusion and disorganization amongst the rebels. As

49 “Turkey timeline: here’s how the coup attempt unfolded.”
anti-government soldiers began to surrender to the police and army, several of them were lynched by angry civilian mobs. In the early hours of the morning, Erdogan gave a televised, then a live address to the people, in which he reaffirmed his party’s control of the country. He accused the conspirators of being linked to the Gulenist movement, which Gulen has categorically denied.\(^{50}\)

In the aftermath of the coup, the AKP declared a state of emergency --- which has yet to be lifted --- that allowed it to take immediate steps to consolidate power and punish those it suspected of involvement. Just one day after the coup was foiled, 2,745 judges were dismissed and detained. As of April 29, 2017 160,000 officials and public servants have been dismissed or arrested on charges of conspiracy.\(^{51}\) The government forcefully seized $11 billion in assets of nearly one thousand allegedly-Gulan-friendly companies.\(^{52}\) Journalists and media outlets seen as critical of the government have been shut down and arrested: 251 journalists are currently under arrest in Turkey, with 24 more having already been convicted.\(^{53}\) The purges have also allowed the government to target the ethnic Kurdish minority, dismissing nearly 12,000 Kurdish teachers and 24 elected mayors, and arresting the co-chairs of peaceful pro-Kurdish political parties for alleged links with the Kurdistan Workers Party.\(^{54}\)

On April 16, 2017, the Turkish government held a referendum on new constitutional measures proposed by the AKP party, which would dissolve the office of the Prime Minister, confer executive power to the office of the President, increase the number of seats in Parliament, and give

\(^{50}\) “Turkey timeline: here’s how the coup attempt unfolded.”
the President power over many judicial appointments. The results, a narrow win (51% to 48%) in favor of constitutional amendment, have been hotly contested by domestic and international actors alike. The Supreme Electoral Council, in an unprecedented move, allowed nearly 1.5 million unstamped ballots to be counted, which opposition parties have alleged benefitted the “Yes” campaign and thus illegitimating the results of the referendum.\(^{55}\) The “No” campaign was denied access to state facilities and funding, and several of its leaders were even subject to violence. Erdogan also accused all “No” voters of being terrorists by siding with the faction behind the failed coup in 2016.\(^{56}\) European election officials have publicly stated that the vote did not meet international standards, and several European countries’ refusal to allow “Yes”-campaign activities and rallies to take place within their borders caused severe international friction with the Erdogan government. Many opposition leaders have argued that the referendum creates, in essence, an “elected dictatorship” by giving excessive power to the office of the president and reducing the power of the legislature.

International reaction to both the governmental response to the coup attempt and the recent referendum has been generally negative. Nearly all allied countries immediately denounced the coup attempt, speaking up for the peaceful transfer of power and respect for rule of law. However, as the post-coup ideological purges began, international opinion began to sour on Erdogan. Then-US Secretary of State John Kerry gave a speech in which he suggested that the Turkish government’s response to the coup attempt could threaten their NATO membership status.\(^{57}\) In the wake of the referendum, key international leaders suggested that the dubious election had all but ended Turkey’s

---


56 Sanchez, Raúl, and Burhan Yüksekkaş.

bid to join the EU, some going so far as to suggest that other EU countries cease funding for Turkey’s membership bid. Erdogan’s pledge, after the referendum, to reexamine the Turkish ban on the death penalty would flout the rules of the European Council, of which it is currently a part, and other member states have expressed concern that this would represent a “red line” that would necessitate Turkey’s removal.

NATO and Turkey’s relationship has been further strained by conflicts in Syria and Russia. The AKP insists that the Kurdish People’s Protection Forces (YPG), a majority part of the Syrian Democratic Forces (SDF), is a terrorist group. The US military had provided arms and training to the SDF in support of their bid to retake Raqqa from ISIL, a move which Erdogan has stated violates the cooperative and multilateral nature of NATO’s mission. Turkey recently purchased an advanced missile system from Russia for $2.5 million, a move which is seen as a sign of its growing frustrations by conflicts over the arming of Syrian rebels and international condemnation of its increasingly authoritarian form of government. Purchasing the system from Russia allows Turkey to circumvent restrictive NATO policies that prohibit the placement of missile defense systems on Turkey’s Greek or Armenian borders. The increasing conflict between the US and Turkey, who possess NATO’s largest and second-largest militaries respectively, has been creating growing apprehension about the future of the alliance and of Turkey’s place within it.

---

Blocs

**USA:** The US is the only power with a military larger than Turkey’s, and the one who has been most in conflict with it over alliances in the Syrian theater. Has also butted heads with Turkey over weapons deals and Russia, and it make seek to punish Turkey for going elsewhere to buy weapons. Likely, its highest priority will be protecting its own strategies and interests in the Middle East.

**France, Germany, Belgium:** Leaders from all three countries spoke out after the referendum to shed doubt on Turkey’s future in the EU and the European Council. Resolution for Turkey’s political situation would free them from an awkward decision about Turkish membership. France and Germany support the SDF like the US, though their contributions are smaller, so Syria is likely to be a bone of contention with these two countries. Especially Germany, and to some extent France, host proportionally large Turkish minorities and thus must consider the domestic impact of their relationship with Turkey.

**Spain, UK:** Two of the strongest supporters of Turkish accession to the EU. The UK and Turkey had historical conflict over the island of Cyprus, but are now strong economic allies. With Brexit, the UK’s stake in Turkish EU membership is less clear, but they remain trade partners with Turkey and thus may not want to rock the boat.

**Hungary, Croatia, Poland, Romania, Slovakia, Slovenia:** EU countries with concerns about the resettlement of Syrian refugees within their borders. May be reluctant to upset Turkey for fear that they will be forced to increase their refugee intake, which is already contentious.

**Albania:** Historical ally of Turkey, who supported its bid to join NATO and continues to provide military support. Highly unlikely to want to chastise Turkey or allow it to leave NATO.

---

61 Hacaoglu, Selcan. “Turkey Chooses Russia over NATO for Missile Defense.”
62 “Turkey Referendum: Key Reactions.”
Greece: Has a tumultuous diplomatic history with Turkey, including a long-standing dispute over Cyprus. Recent relations have been more positive, but comments by Erdogan and Turkish refusal to respect Greek airspace are straining the peace. Likely to push for more punitive action against Turkey.

Norway, Netherlands: These countries are also supporting the SDF in Syria, in opposition to the wishes of the Turkish government, which may create conflict. The Netherlands has a proportionally high Turkish population, so it must maintain a delicate diplomatic balance.

Bulgaria, Canada, Czech Republic, Denmark, Iceland, Latvia, Lithuania, Luxembourg, Montenegro, Portugal: Countries without either strong ties to or points of conflict with Turkey. Likely to prioritize alliance stability over all other factors. Bulgaria and Denmark have a relatively high Turkish population that they must consider.

Turkey: Turkey gains from its alliances and partnerships with NATO countries, but understands that it holds valuable bargaining chips in any negotiation: the size of its military, its strategic location, its resettlement of millions of refugees. Any proposal to change the government or limit Erdogan’s powers will be met with extreme resistance, and a confrontation could make Turkey reconsider the relative advantages of NATO over a partnership with Russia, to whom they have been growing closer in recent years.

---

64 Oltermann, Phillip.
65 Oltermann, Phillip.
• What role, broadly, should NATO have in protecting democracy and freedom across the globe? Need it be more interventionist, or less? How should it define standards of democracy and freedom?

Key terms:

Coup: also known as a coup d’etat, a putsch, or an overthrow, a coup is when the military or another powerful elite seizes control of a state from the existing regime.

Democratic Union Party (PYD): a Kurdish opposition party in Turkey subject to repression by the ruling AKP party, accused of ties to the PKK.

Gulenist: a follower of onetime-AKP-ally Fethullah Gulen, a Turkish preacher who led the moderate conservative Islamic Gulen movement, now considered a terrorist by the AKP regime.

Justice and Development Party (AKP): the current ruling party in Turkey under Erdogan, premised on conservatism and moderate Islam (though its commitment to secularism has been challenged). Has won a plurality in the last five elections.

Kemalism: the founding ideology of the Republic of Turkey, a political philosophy focused on secularism, Turkish nationalism, and westernization.

Kurdistan Worker’s Party (PKK): a leftist Kurdish-nationalist militant organization, fighting an active conflict with the Turkish government for equal rights and increased Kurdish autonomy. Labelled a terrorist organization by the Turkish government and NATO.

People’s Protection Units: a primarily-Kurdish militia that comprises the majority of the Syrian Democratic Forces, the official army of the newly-formed Democratic Federation of Northern Syria which opposes Assad. Labeled a terrorist group by Turkey, but armed and supported by the US.

Purge: the removal, by a regime, of political opponents and dissidents from power, through dismissals or more violent means such as arrests and murders.
**Referendum**: a legislative measure voted upon by the general public, usually passes or fails by a simple majority.

**Questions**

- Does Turkey still meet the membership standards for democracy and human rights that NATO countries ought to uphold? Do these standards apply to existing NATO members? What are other standards that might apply to existing members, if standards for applicants do not?
- If Turkey fails to meet necessary standards, how should the Alliance deal with this? What types of punishment are appropriate and within organizational purview? Sanctions? Expulsion?
- What are the potential consequences of a Turkish departure from NATO? How would the Alliance handle the military and strategic hole that its withdrawal would create (be it voluntary or mandated)?
- How should the Alliance attempt to approach mediating disputes between member countries like Turkey and the US? How should we codify a system of mediation in an organization which cannot force compliance?
- Does the Alliance even have the authority to punish member countries? If so, under what circumstances? In what ways? Does this authority need to be expanded? Should the punitive measures be codified for future disputes?
- Need the Alliance codify membership requirements to minimize ambiguity when situations like these arise (as they are likely to do again)? What would new requirements look like? How would they be judged and enforced?
How much of an interventionist approach should the international community take in the Turkish political system? Are the threats to democracy serious enough to demand international action, and what form would that action take?

Additional reading:

- “How to deal with authoritarianism inside NATO”, War on the Rocks:

- “NATO members are supposed to be democratic. What happens when Turkey isn't?”, Washington Post:

- “Turkey’s Security Challenges and NATO”, Carnegie Endowment:
  - [http://carnegieendowment.org/files/Aybet_Brief.pdf](http://carnegieendowment.org/files/Aybet_Brief.pdf)

- “Turkey’s Slide into Authoritarianism”, Middle East Quarterly:
  - [http://www.meforum.org/6398/turkey-slide-into-authoritarianism](http://www.meforum.org/6398/turkey-slide-into-authoritarianism)

- “Turkish tensions undermine its role in NATO”, Politico:

- “Enlargement”, NATO:
  - [http://www.nato.int/cps/en/natohq/topics_49212.htm](http://www.nato.int/cps/en/natohq/topics_49212.htm)

- “Turkey: History”, Encyclopedia Britannica:
  - [https://www.britannica.com/place/Turkey/Marriage-and-family-life#ref593734](https://www.britannica.com/place/Turkey/Marriage-and-family-life#ref593734)