DISEC BULLETIN

DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE

KELLY YEN, CHAIR
ALEX BLUMENFELD, VICE CHAIR
KEEMIN LEE, VICE CHAIR
## Contents:

Letters from the Chairs ................................................................. 3

**Topic A: Cyber Warfare** ............................................................ 4
  - Introduction ........................................................................ 4
  - Current Situation .............................................................. 4
  - Past UN Action .................................................................. 6
  - Possible Solutions ............................................................. 8
  - Case Studies ....................................................................... 9
  - Questions to Consider ....................................................... 11
  - References ....................................................................... 12

**Topic B: The Syrian Conflict** ................................................... 13
  - Introduction ...................................................................... 13
  - Topic History ..................................................................... 13
  - Current Situation ............................................................. 15
  - Past UN Action ................................................................ 17
  - Bloc Positions .................................................................. 18
  - Questions to Consider ....................................................... 21
  - References ....................................................................... 21
Hello Delegates!

My name is Kelly Yen and I am so excited to welcome you to DISEC at AMUN XVIII. I am currently a senior in the Academy for the Advancement of Science and Technology, and have been participating in Model UN since my sophomore year. This will be my second year chairing DISEC at AMUN and I’m looking forward to hearing all our delegates’ great ideas on this year’s topics. The topics you will be debating have been chosen very carefully and I can’t wait to see what solutions you come up with. If you have any questions or concerns, please feel free to email me.

Sincerely,
Kelly Yen, Chair, DISEC
kelyen@bergen.org

Hello delegates!

I’m Alex Blumenfeld, and I’m excited to be one of your chairs for DISEC this year. I’m a junior in the Academy for Business and Finance, and I’m also on this year’s AMUN Secretariat as Director of Charity Outreach. I’ve been in love with Model UN since my first days at BCA, and I’m serving as Director of Communications for our club this year. Outside of MUN, you can find me doing biology research, competing on our Fed Challenge team and laughing at just about anything John Oliver does.

I was involved with JAMUN, our MUN conference for middle school delegates, during my freshman and sophomore years, and this is my first year chairing at AMUN. I think we have some interesting and thought-provoking topics lined up for DISEC, and I really hope you enjoy the committee. Best of luck!

Sincerely,
Alex Blumenfeld, DISEC Chair
aleblu@bergen.org
Introduction:

The Disarmament and International Security Committee (DISEC) is the first committee of the United Nations General Assembly, which deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime. In addition, DISEC is the main committee within the General Assembly of the United Nations.

Current Situation:

United Nations Institute for Disarmament Research (UNIDIR) defines cyberwarfare as “warfare conducted in cyberspace through cyber means and methods”. These means and methods include cyberattacks and the use of a variety of cyberweapons. The different types of cyberweapons can be divided into three main groups: unequivocally offensive weapons, dual use tools, and unequivocally defensive tools. Examples of unequivocally offensive weapons are malware programs such as viruses, worms, and trojan horses. Dual use tools are processes such as network monitoring and encryption. Unequivocally defensive tools include firewalls and disaster recovery systems. One specific aspect of cyberwarfare that sets it apart from other forms of conflict is the fact that the warfare is conducted in cyberspace, which remains the sole domain that is entirely man-made. UNIDIR defines cyberspace as “a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein”. The current situation concerning cyberwarfare and existing international law can be attributed to certain characteristics of the cyber domain. Cyberspace is maintained, owned and directed by both public and private stakeholders throughout the world and it is a growing domain, due to the constant changes being
applied as technological advancements are made. Furthermore, cyberspace is readily accessible to a large portion of the world including governments, non-state organizations and individuals. It is important to note that while only attacks conducted within the cyber domain would be considered cyberwarfare or cyberattacks, these attacks could possibly produce effects outside of cyberspace.

The laws and policies applied to cyberwarfare has been questioned in terms of international relations. According to the UN Charter, cyber operations utilizing force are prohibited, as stated in Article 2 of the charter. However, this article was solely addressed towards states. Therefore, in order to prohibit the use of threats or force within cyberspace, these actions must be attributed to states and directed against at least one other state. In order for actions to be attributable to states, international law dictates these actions buts be performed by someone acting on behalf of the state, or with the authorization of the state. With that authorization comes the state’s legal responsibility to be attributable to actions concerning international law.

A large part of the current situation regarding cyberwarfare can be attributed to the advanced technology that is utilized to control and maintain critical infrastructures throughout the world. Through cyberattacks, any country could possibly access the control systems of critical infrastructures of any other country, which could have drastic repercussions. An attack on critical infrastructures could be perceived as an “armed attack”. This would allow the country being attack would be to forgo any restrictions outlined within the UN Charter and take up self-defensive action. This leads to further arguments as to what defines an “armed attack” and what defines “critical infrastructure”. In a 2005 UN General Assembly resolution, critical infrastructures were defined as “those used for, inter alia, the generation, transmission and distribution of energy, air and
maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations”. The United States has referenced many definitions of critical infrastructures in acts and directives throughout the years. For instance, in the 1998 US Presidential Decision Directive 63, titled “Critical Infrastructure Protection”, it states, “Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private”. Later in 2003, The White House issued “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,” in which they stated, “The critical infrastructure sectors consist of agriculture and food, water, public health, emergency services, government, the defense

industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping”. Though the UN General Assembly called for each country to determine its own definition of critical infrastructures, the ambiguity of the term could possibly affect how cyberattacks are identified and dealt with.

Past UN Action:

In 2012, UN Secretary-General Ban Ki Moon appointed a group of experts to research and report their findings on the subject of information and telecommunications, specifically concerning international security. The 15 experts came from a variety of countries including the five permanent members of the UN Security Council, China, France Russia, the United Kingdom and the United States, as well as Argentina, Australia, Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan. The primary goal of the group was to “study possible cooperative
measures in addressing existing and potential threats” related to information and communications technology (ICTs), as directed by the UN General Assembly. In their report, the committee of exports sought to clarify which rules of warfare were applicable in cyberspace, as that was identified as a large factor contributing to instability, the risk of escalation, and the possibility of mistaken cyberwarfare. As stated within the report, it was affirmed that international law, specifically the principles of the UN Charter, would be applicable to any state activities within cyberspace. These activities included the activities of non-state actors which would be attributed to state. This affirmation was made in order to ensure the international community and any involved states would react to violations of international law within cyberspace more effectively. For instance, as specified in Article 51 of the UN Charter, a state holds the right to selfdefense through the use of force under the conditions that a cyberattack reached the level of an “armed attack”. Russia was one of the notable countries who accepted the application of international law to cyberspace, while China stated it felt that such actions and statements were premature and an opposition to the objective of preventing the spread of offensive cyberweapons.

A different study, which was conducted by UNIDIR, found that over 40 UN member states have developed some form of military cybercapabilities. 12 of these member states have developed cybertechnology specifically for offensive cyberwarfare.

At the 39th annual Group of 8 (G8) summit meeting in June 2013, it was jointly announced by US President Barack Obama and Russian President Vladimir Putin that Russia and the US had established the first-ever bilateral agreement concerning cybersecurity and security measures within the cyber domain. The agreement was focused on information exchange and crisis communication. Within the agreement, three cyberspecific crisis communication channels were established. One of the channels was between computer emergency response teams (CERTs) from both Russia and the US to discuss malware that may originate from the other’s territory. A telephone hotline between the White House and the Kremlin was established in the case of a major cyberincident. Lastly, a link was formed between nuclear risk reductions centers for cyberincidents that are deemed
important at the national security level. This bilateral agreement between the two countries was affected by the tense relations between the US and Russia since 2014, during which Russia invaded eastern Ukraine and annexed Crimea. Since then, Russia has been suspended from the G8 therefore preventing the cybersecurity agreement to be carried out. Following the cyber attack that targeted a portion of a Ukrainian power grid in December 2015, many US security officials believed that Russia was behind the attack. In attempts to prevent the US and Russia from mistakenly creating a cyber war, the two countries held meetings in April 2016 in order to discuss the attack on Ukraine. US officials made a statement about the meetings in which they said, “This meeting is not a restart of the Bilateral Presidential Commission working group (suspended in 2014 after Ukraine) but it is in our interest to discuss cybersecurity issues with Russia, including to review the 2013 Bilateral US-Russia Cyber (confidence building measures).”

Possible Solutions:

The report from the group of experts appointed to “study possible cooperative measures in addressing existing and potential threats” related to ICTs, the following confidence-building measures on state behavior in the cyber domain were recommended:

Exchanging information on national policies, organizations and structures, good practices, and certain processes when concerning cybersecurity. For instance, the United States exchanged white papers about the subject of cyberdefense with Russia in 2012. Similarly, Germany conducted an exchange with Russia in 2013.

Creating bilateral or multilateral agreements about cybersecurity and managing the cyber domain. In example, the US established the first-ever bilateral agreement concerning cybersecurity with Russia in 2013, as detailed in the “Past UN Action” section of this topic guide.

Increasing cooperation among states to address cyberattacks against critical infrastructure systems, specifically those that are controlled and maintained by
ICT-enabled industrial systems, and establishing more crisis communication between states concerning cybersecurity incidents. The resolution titled “Developments in the field of information and telecommunications in the context of international security” can be found here:


Case Studies:

OPM HACK

In July 2015, it was revealed that a cyberattack had breached the computer systems of the Office of Personnel Management (OPM) and had resulted in the theft of the personal information of approximately 21.5 million people in the US. This personal information included the Social Security numbers, addresses, health and financial history, fingerprints and other private details of every person who had received a government background check within the 15 years prior to the cyberattack. It was determined that approximately 19.7 million of the victims of the cyberattack had been applicants for security clearances within the US government while the 1.8 million others had been their relatives, spouses or friends. Allegedly, the hackers had access to the OPM databases for over a year, allowing them to go through the systems and networks therefore establishing the breach as a possible threat to national security. These attack caused more questions to be posed about the strength of cybersecurity within the US government systems and networks.

Following the attack, many government officials questioned the vulnerabilities of the federal networks and called for greater security measures to be taken when concerning important federal information. For instance, the White House cybersecurity coordinator, Michael Daniel, called for a raised level of cybersecurity within both the public and private sector. Furthermore, James B.
Comey, Jr., the director of the F.B.I., addressed the severity of incident and stated, “There is a treasure trove of information about everybody who has worked for, tried to work for or works for the United States government. Just imagine you are an intelligence service and you had that data, how it would be useful to you.” The breach also fueled the debates within Washington over how to handle the weaknesses of US cybersecurity, leading to a call from both parties of Congress for the resignation of Katherine Archuleta, the director of OPM. Following the breaches, OPM announced new security measures would be put in place, as well as free credit and identity theft monitoring for anyone who may have been affected by the cyberattack.

A related breach occurred just a month prior in which the data of 4.2 million federal employees was compromised, as reported by OPM. The two breaches were believed to have originated in China and established the largest cyberattack on US government networks, therefore causing concerns about the technological security of federal agencies who deal with sensitive information.

UKRAINE

Just this past December, a portion of the Ukrainian power grid was attacked by sophisticated cyberattack techniques which triggered a power blackout, possibly the first ever triggered by a cyberattack. Prior to the cyberattack, the attackers studied the networks that controlled the power grid, stole credentials from system operators in order to gain access, and learned how to switch off the breakers therefore triggering a blackout affecting over 225,000 Ukrainians.

The specific malware used in the attack was created to attack industrial control systems which function as the links between computers and infrastructure controls such as machinery that is used to mix chemicals and switches that are used to distribute electricity. Investigators say that the attack on Ukraine could have had an even worse effect if not for the fact that the country still utilizes
old technology, allowing them to restore power to the power grid through manually flipped circuit breakers. This has led to questions about the vulnerability of the United States electric grid. According to Ted Koppel, the author of “Lights Out”, a book focused on the vulnerability of US electric systems, “[America has] 3,200 power companies, and we need a precise balance between the amount of electricity that is generated and the amount that is used. And that can only be done over a system run on the Internet. The Ukrainians were lucky to have antiquated systems.”

Following the cyberattack, the Obama administration warned utilities companies such as power companies, water suppliers and transportation networks, as they could be possible targets for future cyberattacks. Cyberattack targeted towards critical infrastructures could be very damaging to any country with advanced technology and network control systems.

**Questions to Consider:**

1. Could utilizing cyberwarfare benefit countries? If so, which countries seek to the gain the most by conducting cyberattacks.
2. How does the ambiguity regarding cyberwarfare and international law allow for countries to conduct cyber warfare with no restrictions or repercussions?
3. How should safeguards inspections be conducted in order to respect national sovereignty and intellectual property rights?
4. How should the committee deal with hackers conducting cyberattacks but not on the behalf of their country?
5. How could the committee prevent countries from hiring third party hackers
to conduct their cyberwarfare?

6. How will the advancement of artificial intelligence affect cyberwarfare?

References:

2. https://www.armscontrol.org/act/2013_09/TheUN-TakesaBigStepForward-onCyberssecurity
   rref=collection%2Ftimestopic%2FCyberwarfare&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=21&pgType=collection

Introduction:
What we now know as the Syrian Civil War began in 2011, with a series of protests at the peak of the Arab Spring movement. However, the situation quickly got violent, and full-on conflict was soon ignited between the military of Syrian President Bashar Assad and opposition fighters seeking to take him out of power. The fighting quickly escalated, and it has proceeded to take over Syria, displacing millions of Syrians and killing thousands. President Assad has been widely criticized by the West for his authoritarian policies, such as employing his secret police to intimidate political opposition and imprisoning dissidents. Assad and his government are Alawites, a Shia minority, which puts them even further at odds with the mostly Sunni rebels while giving them a de facto alliance with predominantly Shia Iran. Many countries have criticized Assad’s regime and would like to see him leave power in favor of a democratically elected transition government, but there has been limited external military action against Assad so far by powers such as the United States, the United Kingdom, and Saudi Arabia.

Although they are allied against ISIS, as will be discussed shortly, they have not shown as clear a military commitment against Assad. For now, there are a variety of rebel groups fighting Assad, but he still remains in power.

**Topic History:**

To make matters worse, pro-regime soldiers and anti-Assad rebels are not the only parties fighting in Syria: there is also the problem of the exceptionally dangerous terrorist organization the Islamic State in Iraq and Syria, or ISIS. In the name of establishing an Islamic caliphate, ISIS has claimed a wide swath of territory across northern Syria and central Iraq (to clarify, this committee will only be focusing on ISIS’s activity in Syria, not Iraq). They have horrified civilians around the world with their much-publicized beheadings and desire to convert as much of Syria as possible to Sharia law, but the real reason why so many countries are concerned about their existence is their presence as an international
terrorist network. From the mass shooting in Orlando to a bus running into a crowd of civilians in Nice, ISIS has claimed responsibility for a number of high-profile attacks, which makes them a direct threat to the national interests of countries such as the United States and France in addition to Syria and Iraq. Although they are not officially allied, Assad and ISIS have cooperated at times, which makes both of them even more dangerous in the eyes of their enemies.

The main group fighting ISIS in Syria at the moment is a United States-and Saudi Arabia-led coalition of Western and Gulf states’ militaries, which has made some slow but steady progress in the region. In the words of the United States government, the coalition has three main objectives in destroying ISIS: carrying out airstrikes, training local rebels and security forces and completing a variety of other special operations missions. They have proceeded to launch over 10,000 airstrikes that have pushed ISIS back from several key cities, but there is certainly much more work to be done. Although it has been acknowledged by several participating governments that this war cannot solely be won with airstrikes, the coalition’s military efforts are still a valuable component of efforts against ISIS.

There is also the question of the involvement of the Kurdish military, as they are one of the few parties achieving major successes against ISIS but also have quite controversial motives. The Kurdish militia, known as the peshmerga, is combating ISIS in northern Syria as well as pro-Assad forces, and they have made a lot of good progress (mostly against the Islamic State), but not without casualties. The Kurdish groups fighting ISIS have long desired an autonomous state (they already occupy territory in northern Syria and northern Iraq), but that dream has not been realized yet, which may become an issue when foreign powers continue to attempt to collaborate with them against ISIS. Although the Kurds do have a substantial amount of territory and an already semi-autonomous state, they are despised by Turkey, which has repeatedly bombed them, limiting progress in the battle with ISIS. They have gained support from the
United States and other coalition members, but they are also controversial because of their connections to a variety of extremist groups (not ISIS), most notably the Kurdistan Workers’ Party, or PKK. The left-wing PKK has been outlawed in Turkey for years because of its pattern of attacks and violence against innocent civilians, and it is still a safety concern in Turkey - in fact, the United States, the United Kingdom and the European Union have all labeled the PKK a terrorist group. The main Kurdish group in Syria, the Workers’ Protection Units (YPG), have also been condemned by Turkey’s government, but because of their success against ISIS, they are not viewed as badly by most nations. Of course, Turkey isn’t exactly the model anti-ISIS force either: although they technically oppose ISIS and allow other nations to use a key air base to launch strikes against ISIS, they have a record of allowing foreign jihadist fighters to slip through their borders and travel to Syria to fight for the Islamic State. In addition, their practice of bombing both ISIS and the Kurdish militias makes them one of the most controversial players in the Syrian Civil War.

**Current Situation:**

It is extremely important to realize that one of the biggest fallouts from the Syrian conflict has been the resulting refugee crisis, which has already impacted millions of civilians and is slowly pulling the European Union apart. More than ten million people have been displaced, both internally and externally, within Syria since the initial protests first began, and the fallout has been catastrophic. The refugee crisis has deep roots in the political and economic instability characterizing modern Syria, and it will certainly not be easy to solve. As much of Syria is turned into a giant battlefield, many Syrians are constantly at risk or under fire, and they have found that the best way to live their lives is to leave home in search of a better future elsewhere, either in another part of Syria or in the EU. In addition, the collapse of the Syrian state is devastating the economy, hurting business owners and causing big economic problems that are also having negative
impacts on many Syrians. Of course, at the most basic level, the foundation of the refugee exodus from Syria is the lack of widely available food and drinking water, a clear factor in many families’ decision to emigrate. However, the situation is not much better in refugee camps, which are substantially over capacity and simply do not have the resources to provide for the millions of refugees looking to them as their only way out of the conflict zone. Particularly, camps in Greece and Italy (at the southern end of the EU) have been overwhelmed with asylum requests, creating a very unmanageable situation with the current resources. European countries have not been able to take in a large percentage of the Syrian refugees accumulating at their borders, making the situation even worse for those civilians who can only simply wait and see if their request will be approved at some time in the future.

In addition to the current status of Syria’s refugees, the actual conflict in Syria has been rapidly evolving, with the anti-ISIS coalition and Kurdish forces finally starting to make some progress against ISIS. However, the Islamic State is still a huge threat, with built-up economic operations and the ability to carry out attacks all over the world. The number of attacks for which ISIS has claimed responsibility, or at least those that are widely reported on, seems to have been increasing recently, and counterterrorism agencies are still struggling with this new threat. This is partly due to ISIS’s strong internal government and its many methods of raising revenues to fund their wars against the coalition/Russia/the Kurds and their terrorist operations abroad. ISIS has shown itself to be unique among terrorist groups in that it has created an organized state as opposed to a weakly connected network of smaller extremist groups. ISIS controls public services like electricity in territory it has captured, and it imposes a tax system on civilians living in its territory in exchange for safety, water, power and other important services. This is a large part of how ISIS finances its various ventures, but they do have several other sources of revenue, two of them being artifact sales and oil fields. As
Syria is a historic region with many ancient and sometimes religious artifacts, ISIS has been able to pillage its territory to find valuable pieces that they can sell on the black market for millions of dollars. In addition, ISIS has also been able to sell the oil from local reserves, although the coalition and its other enemies have realized that and have begun launching airstrikes on those valuable fields. The Islamic State has been using its continually accumulating cash to buy huge quantities of weapons, among other things. Obviously, any plan to combat ISIS must include a strategy to disable its economic apparatus, in addition to measures to reduce its ability to import and transport arms. As an example, Turkey’s weak border security and questionable commitments to taking down ISIS make it very easy to ship weapons into ISIS hands in Syria.

Although ISIS has been getting a lot of headlines recently, President Assad is just as essential as ever to the conflict in Syria. Pro-regime forces continue to fight it out with several rebel groups, although the fight appears to have shifted in Assad’s direction: from the current situation, it does not appear as though the rebels have the capacity to deal a crushing blow to his authority at the moment, but the situation is of course still rapidly evolving. As millions of civilians are being caught in the crossfire and the entire region is being destabilized by Syria’s wars, it is essential that this committee deal with both President Assad and ISIS to create a sustainable future for a region desperately in need of peace.

**Past UN Action:**

The UN has taken a wide range of actions on Syria already, but they have clearly not solved the crisis yet. Specifically, its resolutions have focused on topics such as condemning President Assad’s use of chemical weapons, calling for a political solution to the Syrian crisis and fair elections, increasing counterterrorism efforts in the region and providing humanitarian aid to those in need. First, the OPCW-UN Joint Mission in 2014 successfully confiscated large quantities of chemical weapons from government facilities and the mission was deemed complete, but President Assad’s
forces are still using weapons such as chlorine bombs in violation of past UN resolutions. This case is the first time chemical weapons have been used in a country that is a party to the Chemical Weapons Convention, which would appear to cast doubt on the UN’s ability to prevent these attacks. This was addressed in March 2015’s Security Council Resolution 2209, which continued to condemn Syria’s use of chemical weapons and promised that “individuals responsible for any use of chemicals as weapons...must be held accountable”, conceivably referring to President Assad.

The UN has also recognized the dire humanitarian situation in Syria, reflected in its decision to allow UN agencies and their partner NGOs to cross conflict lines and use several key border crossings into Syria to provide aid and medical supplies to civilians. The Vienna Process, the UN’s primary mechanism of Syrian diplomacy, has agreed to authorize World Food Programme airdrops to civilians in the near future, as safe ground routes to areas in need have often been hard to come by. Several ceasefires have failed over the past few years, and the UN, the United States and Russia have had difficulty getting all parties to agree on a temporary peace for humanitarian relief.

Finally and perhaps most importantly, the UN has repeatedly shown a commitment to a peaceful political transition in Syria and it has made several attempts at sustained peace talks between all parties involved in the conflict. Various attempts at peace have been made since 2011, but without much success. The Vienna Process has made limited progress, but has currently stalled without deciding on a political solution to Syria’s crisis or even a date to resume talks. Resolution 2254 set a goal of having free and fair elections in Syria 18 months after its passing, which puts the UN’s proposed deadline for instituting a fair political process at June 2017. However, given the current state of affairs in Syria, it has yet to be seen whether this timeline will be followed.

**Bloc Positions:**

**THE UNITED STATES OF AMERICA**

The United States is most concerned with counterterrorism and the demise of ISIS, and
although they have reiterated that they will not accept a future in which President Assad still rules Syria, they have so far not shown willingness to make that happen, evidenced when Assad was not penalized for crossing Barack Obama’s “red line” of continuing to use chemical weapons. The US is leading the coalition against ISIS and views the organization as a huge threat to national interests, and they have attempted to train and supply “moderate rebels” in Syria to attack ISIS, with limited effect. Although America has so far not committed a large number of ground troops to the operation, it should be noted that their priority is on ISIS, which contributes to their focus on domestic counterterrorism operations.

EUROPE

For the most part, the European Union is similar to the United States in that it mostly dislikes Assad and is very concerned about the rise of ISIS. However, the EU faces a problem that America does not: the refugee crisis caused by Syria’s civil war. Many European nations, especially those on its southern end, have been overwhelmed by the influx of refugees coming in from Syria and would likely favor any sort of arrangement that brings peace to Syria, in order to stem the tide of migrants. Many Europeans also believe that the crowds of refugees are full of terrorists, which makes them even more predisposed against them. Even the European country most friendly to refugees, Germany, has started to shift away from that stance, so it can reasonably be said that Europe is committed to ending the flow of refugees, whether that comes through sustained peace in the region or humanitarian aid that prevents Syrians from having to leave their homes.

RUSSIA

Russia has been one of President Assad’s strongest allies for decades and has assisted the Syrian government by launching airstrikes on rebels fighting Assad’s forces. Although this would put them at odds with many other powerful nations (ex. USA, UK), Russia has also used its air force to strike at ISIS, regarding both the
Islamic State and the rebels as their enemies.

However, President Putin has pledged to begin pulling his troops out of Syria, and he has previously stated that the only way to end the conflict in Syria is a political solution, which would appear to be bad news for Assad. Russia has been willing to collaborate with the United States and the US-led coalition against ISIS, but their stance on Assad definitely sets them apart from the coalition.

SAUDI ARABIA

Saudi Arabia (ruled by Wahhabis, a Sunni sect) has been one of Bashar Assad’s major critics and is committed to removing him from power, whether by peaceful transition or by force. They have provided weapons and funding to several rebel groups, and they are eager for the United States to begin a larger military operation against Assad. Saudi Arabia was not originally particularly concerned about ISIS, but their policy has changed recently and they are now one of the key nations participating in US-led airstrikes against the Islamic State.

TURKEY

Turkey has one of the most controversial stances on the conflict in Syria: they are staunchly anti-Assad and anti-ISIS, yet they are also cracking down on the Kurds, one of the few groups enjoying substantial success against ISIS. Turkey’s effectiveness in combating ISIS is also called into question by its loose border policies and tendency to allow foreign fighters to pass through the country on their way to Iraq or Syria to fight for ISIS. Turkey is also facing a new level of instability due to the recent attempted military coup, but nevertheless, they are an important component of the fight against both Assad and ISIS due to their proximity to Syria and their resources.

IRAN

Iran is another of the Assad government’s allies, as they are a majority-Shia nation, and they have fulfilled that responsibility by providing large amounts of military supplies, loans and oil. Iran needs
Syria in order to ship weapons to the Lebanese extremist group Hezbollah, and they have also provided troops to fight with Assad on multiple occasions. However, Iran is also working to push back ISIS, which puts them in an interesting position between the United States and the coalition on one side and Assad and Russia on the other. Iran favors a political solution to create a more stable government and previously voiced its desire for free elections in the near future, but they are still close allies of President Assad.

Questions to Consider:

1. Should the main focus of military efforts be on taking down Assad or on pushing back ISIS? Which is the lesser of the two evils?
2. How can this committee cut off non-military ISIS operations such as the sale of captured oil and the continued influx of foreign fighters?
3. Is President Assad part of the region’s future? Should this committee work toward a future in which ISIS has left Syria, but Assad is still in power?
4. Is a political solution to the Assad conflict viable, or is a full-scale military intervention the only way to create a viable Syrian government?
5. Should the Kurdish militias be given support because of their success in combating ISIS or punished for their affiliation to a terrorist Turkish political party?
6. How can this committee reduce the conflict’s effects on refugees, children and other vulnerable groups?

References:


