PacificMUN 2017

North Atlantic Treaty Organization (NATO)

Backgrounder Guide

Topic B: Cyber Defence

PacificMUN 2017

Dare to Speak | February 24–26 2017

Bryan Buraga
Secretary-General

Christopher Yuen
Deputy Secretary-General External

Timothy Ro
Deputy Secretary-General Internal

Alice Li
Chief of Staff

Elizabeth Vaz
Under Secretary-General of Delegate Affairs

Charles Balcita
Under Secretary-General of Committees 1

Alan Milligan
Under Secretary-General of Committees 2

Saad Yasin
Under Secretary-General of Conference

Jonathan Kim
Under Secretary-General of Finance

Shakil Jessa
Under Secretary-General of Sponsorship

Andy Wang
Under Secretary-General of Information Technology

Mingxin Gong
Under Secretary-General of Design and Media

Dear Delegates,

My name is Woojin Lim and I am very delighted to serve as the director for the North Atlantic Treaty Organization (NATO) at Pacific Model United Nations 2017.

First and foremost, I would like to extend a warm welcome to all delegates who have chosen to serve as one of 28 member nations in NATO. I can assure you that it will be a memorable experience exploring the geopolitical and military standpoints of allied nations, debating topics regarding the future of the alliance's strategic Eastern front and the progression of collective cyber defence, and working with each other to bridge consensus over the given resolutions.

Experienced in university-level Model NATO, I will try my best to make an authentic atmosphere most representative to the actual NATO.

A little bit about myself: currently, I am a junior student attending Fraser Heights Secondary. I am an avid public speaker and debater who is passionate about international relations, social justice, and criminal law. Since last year, I have rekindled my interest in Model United Nations and have reappeared in the MUN community as a delegate, and now a staff member.

On behalf of my chair Nathan, I once again extend a warm welcome to all NATO delegates at PacificMUN 2017.

Sincerely,
Woojin Lim
NATO Director
PacificMUN 2017

The North Atlantic Treaty Organization (NATO) was originally established on April 4th, 1949 as an intergovernmental military alliance between 12 founding member states to prevent the proliferation of communist ideologies of the former Soviet Union (USSR).[1]

Since the collapse of the USSR in 1991 at the end of the Cold War, although NATO lost its historical purpose for having existed, NATO has transitioned its goal to safeguarding the freedom and security of its current 28 member states in Europe and North America. Outlined by NATO's 2010 Strategic Concept, the three fundamental objectives of the North Atlantic Alliance, created for the purposes of safeguarding Alliance members in the interests of international law, include, but are not limited to: (1) the guarantee of collective defence as a primary mechanism of defence amongst member nations, (2) the continuation of overseas crisis management of issues that potentially undermine the interests of the alliance, and (3) the provision of cooperative security amongst neighbours and international partners on grounds of common concern.[2] As enshrined in Article 4 of the Washington Treaty, NATO uniquely remains as the sole organization in which parties collectively come together to discuss all issues of contention that impact the territorial integrity, political, independence and/or security of its members.[3]

Aside from its primary goal to protect the members of the organization through means of diplomacy, and if necessary military force, NATO also strives to achieve global peace. Without the looming threat of the USSR after the Cold War, NATO began to conduct peacekeeping operations in the formerly communist territories, namely during the Bosnian War in 1992, then the Kosovo Conflict in 1999. Operating under the principle of collective defence, as reinforced by single most important Article 5 of the Washington Treaty (which was invoked for time by the United States following the 9/11 terrorist attacks). NATO undertook measures to mitigate the threats posed by terrorism in enhancing intelligence-sharing and cooperation. Similarly, although not an Article 5 action, many members of NATO are currently involved in the coalition against the Islamic State of Iraq and Syria (ISIS) and the continuous fight against terrorism.

Recently, the six-decade old military alliance was once again called to take action following the annexation of the Crimean Peninsula by the Russian Federation on March 18, 2014.[4] For the first time since the cold war, conventional warfare was once again a topic of discussion. Russian-NATO tensions rose, as Russia began to conduct massive military exercises within its

[1] http://www.nato.int/cps/en/natolive/topics_52044.htm
[2] http://www.nato.int/strategic-concept/
[3] http://www.nato.int/cps/en/natolive/official_texts_17120.htm
[4] http://www.nato.int/cps/en/natolive/topics_50090.htm

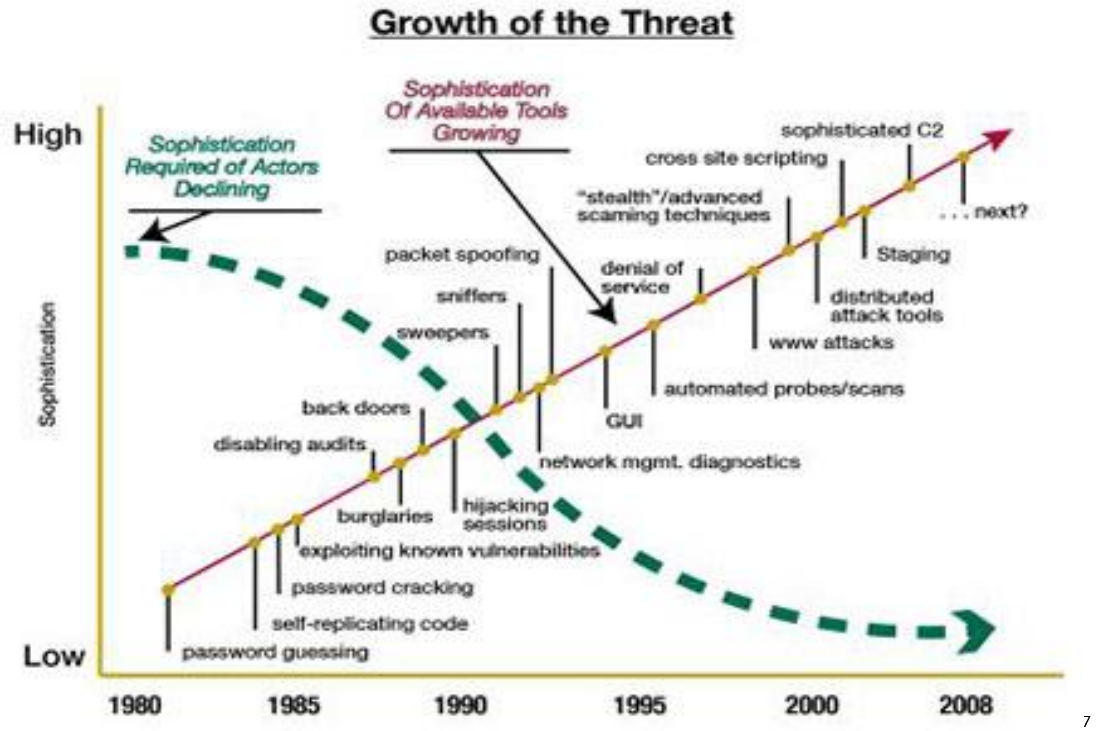
borders.[5] Yet in the 21st century, aside from the usage of guns and tanks, expert hackers hired by intelligence agencies of a plethora of countries, as well as independent groups, threaten to infiltrate the privacy of NATO's databases. While espionage and counterespionage no longer occurs physically; they both have become cyber concepts. Faced with two imposing threats, NATO held the Warsaw Summit from July 8th to July 9th, 2016, in order to strengthen its defence both militarily and digitally.

NATO has always been regarded as the champion of the Western World, bringing stability and security to all of its member states and beyond; at PacificMUN 2017, that responsibility lies in the hands of the delegates. As a concerted body, you will hold the lifeline of not only the 28 members of this organization, but also the entire democratic world that depends on the protection of the West. Succeed, and the ideals and stability that NATO stands for shall survive and thrive; fail, and the world will face an impending shift of power, and out of the ashes may rise a totalitarian order. Act wisely, and the future shall be bright.

[5]https://www.thenation.com/article/the-united-states-and-nato-are-preparing-for-a-major-war-with-russia/

In NATO's Strategic Concept for the Defence and Security 2010, NATO accurately predicted the threat of cyberspace: "Cyber attacks are becoming more frequent, more organized and more costly […]; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability."[6]

The Internet has been a rapidly growing platform which has allowed for the interconnectedness of the international community. It has provided individuals, communities, countries, and organizations the ability to store and search up a vast range of information from all over the globe. Although there exists a plethora of benefits due to the existence of the Internet, at the same time, dangers inevitably remain. Among these harms include the ability of individuals to hack into technology systems to steal valuable information, branch security, commit technological terrorism, and interfere with communications, which could result in the vulnerability of a state's national security. Cyber crimes are difficult to track defend against, and thus, requires the improvement of NATO's cyber security mechanisms.



[7]

The potential threats of cyber attacks have grown alongside the progressive evolution of modern technology

The International Technological University defines cyber security as: "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies […] used to protect the cyber environment and organization and user's assets,"[8] in order to ensure the "attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."[9] In this case, concerning issues that may affect the leakage of classified information, interruption of vital services, and issues that may affect collective security.

[6] http://www.nato.int/cps/en/natolive/official_texts_68580.htm
[7] http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/
[8] http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.
[9] Ibid

1982	The United States of America successfully initiates a proto-cyber attack that reprograms computer equipment, in order to make a Soviet gas pipeline explode.[10]
1988	Robert Morris, a 22 year old student at Cornell University, creates the world's first computer Internet worm, known as the Morris worm, which spread to 6000 computers, slowing them down to a point in which was unusable.
2006	Unknown foreign intruders gained access to the latest US space launch vehicles, which forced NASA to block emails with attachments.
2007	Unknown foreign intruders invaded Estonia's online government networks, resulting in the temporary shutdown of online banking and other government services.
2008	During the time of the Georgia-Russia conflict, Georgian computer networks were hacked by unknown foreign intruders; although there was not a disruption in services, graffiti appeared on the government website.
2009	During the military involvement in the Gaza Strip, unknown foreign intruders hacked into Israel's internet infrastructure and government websites.
2011	A cyber attack on the Canadian governmental agencies, including an agency for Canada's Department of National Defence and the Finance Department and Treasury Board, caused them to be disconnected from the Internet.
2012	Kaspersky, a Russian firm, found that a world-wide cyber virus called "Red October" had been collecting information from "government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures"[11] since 2012.
2013	The South Korean government reported their broadcasting networks, including YTN to be infected from cyber attacks from North Korea.
June 4, 2013	NATO held their first meeting regarding cyber defence, where NATO Defence Ministers made a commitment to cyber defence and relevant capabilities, "extending protection to all the networks owned and operated by the Alliance."[12]
2015	Chinese hackers were deemed responsible for the wide-scale hack on the United States Office of Personnel Management, which leaked over 20 million government employees' information.

[10] https://gcn.com/articles/2013/05/30/gcn30-timeline-cybersecurity.aspx
[11] http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
[12] Ibid

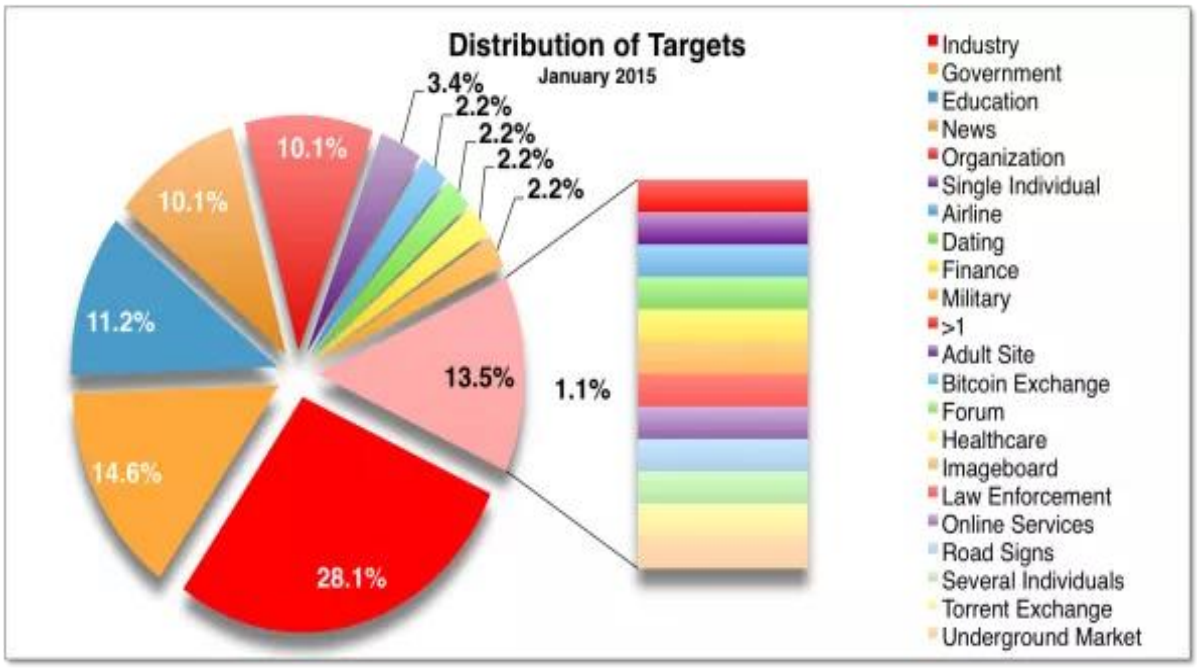
The main crux of NATO's cyber defence policy started formulating after the 2007 cyber attack on Estonia. Starting from April 27, 2007 and lasting for over three weeks, unknown foreign intruders, who were later revealed to be Russian sympathizers that wanted the removal of a Soviet statue from Tallinn (the capital of Estonia), invaded Estonia's prominent government and corporate networks, including the Estonian parliament, ministries, newspapers, and banks. Some of the sustained Distributed Denial of Service (DDoS) attacks were carried out with ping floods, while other attacks were conducted by rented botnets. Although it is known as one of the most wired countries in Europe, Estonia suffered severe damages from the disruption of essential government services and the temporary shutdown of online banking.[13] This was the first time a country requested NATO assistance in defending a cyber attack. As an attack of this nature has not occurred before, NATO was unprepared as it was only experienced in protecting its own networks and communication systems. Taking note of the devastating consequences, NATO has since begun to shape its policies on cyber defence, developing the ability to assist members and partners on the issue of cyber attacks.

Aimed at slowing down Iran's nuclear program, in 2009, the United States' National Security Agency, Central Intelligence Agency, and Israel allegedly built the Stuxnet computer worm, which destroyed roughly 1000 of the 6000 Iranian Siemens uranium enrichment centrifuges. On the eve of the Holocaust Remembrance Day on April 7, 2013, there was a coordinated cyber attack by anti-Israel groups, who attempted to "erase Israel from the Internet" through attacks aimed at the denial of service, administration panel takeover, and database hijacking and leaks. Although this scheme, known as #OpIsrael, caused no significant security-breaches, several websites were taken down or defaced. It has been reported that this attack has been taking place annually since 2013.[14] A situation that showed the devastating financial impacts of inadequate cyber security was the cyber attack against Target in December 2013, where over 40 million shoppers were robbed of their credit and debit card information. After the incident was publicly announced, Target lost 46% of its profits and had to pay over $10 million in damages. In 2014, leading up to Russia's annexation of Crimea, Russia and Ukraine conducted cyber attacks against each other. In December 2015, Russia attacked Ukraine's electric grid, which left around 230,000 residents with no electricity for up to 6 hours.[15]

As the cyberspace continues to expand, the potential dangers and threats of cyber attacks increases alongside it. Not only do these examples clearly demonstrate a growing threat to European security from an increasingly aggressive Russia, but also allows room for other nations or organizations, not limited to the hacktivist/terrorist group Anonymous, China, Iran, and North Korea, who may have the intention and capability, to carry out malicious cyber attacks that can threaten the security of NATO.

[13] http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/
[14] http://www.recode.net/2016/4/7/11585928/anonymous-hack-israel-day-could-impact-the-entire-world
[15] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Recent talks on NATO's new strategic concept have discussed the importance of cyber defence. NATO heavily relies on its cyber space to perform operations and store classified information. Just as other institutions that rely on modernized technology to perform their services experience an increase in cyber attacks, likewise, NATO is experiencing a greater frequency in the number of cyber attacks: from common, small-scale malware causing problems to the temporary discontinuance of public services or the robbery of classified data.



[16]

Worldwide cyber attack statistics showing the distribution of targets

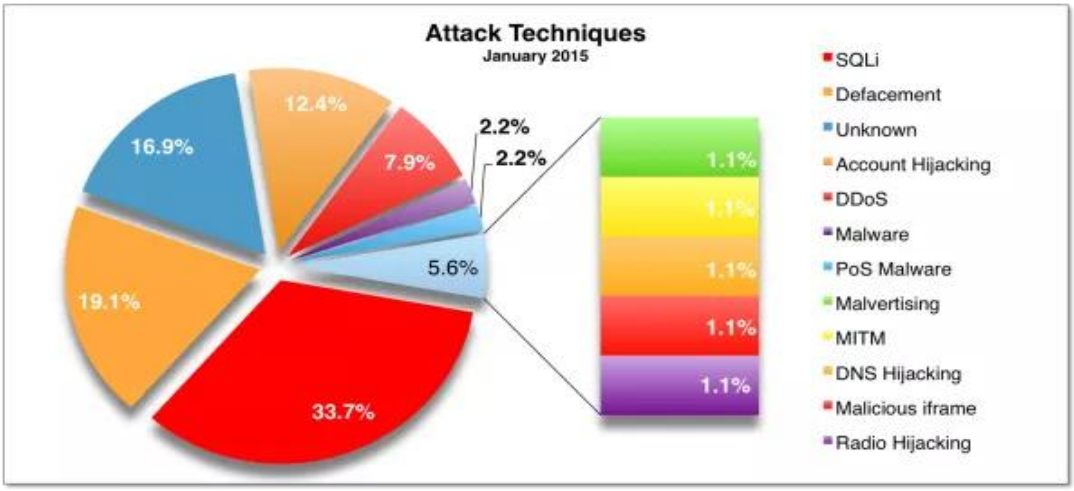
In May 2010, the 13th NATO Cyber Defense Workshop was held, bringing technology and security experts together to discuss ways of protection against cyber attacks. Along with the *Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, the workshop discussed topics ranging from international cyber security to cyber war and the legal parameters of cyber defence to remedies for cyber attack victims. During the workshop, the Estonian Defence Minister Jaak Aaviksoo explained that "every NATO country needs to develop a national approach to cyber security that encompasses all important stakeholders."[17] Aaviksoo then continued to highlight that the ones most vulnerable to cyber attacks are the private sector in NATO nations, where most of the infrastructure exists. Finally, he outlined the significance of developing partnerships. Soon after the workshop, NATO published "NATO 2020," a comprehensive document that regarded NATO's new strategic concept, which outlined the

[16] http://www.hackmageddon.com/2015/02/05/january-2015-cyber-attacks-statistics/
[17] http://www.nato.int/cps/en/natolive/news_63989.htm?selectedLocale=en

importance of "[accelerating] efforts to respond to the danger of cyber attacks by protecting its own communication and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defense capabilities aimed at effective detection and deterrence."[18]

The issue reappeared in light after Chinese intruders made hacks against American government offices and businesses. In June 2015, the United States Office of Personnel Management was reportedly targeted through a data branch on personally identifiable information---one of the largest branches of federal data in American history. By July 9th, 2015, the number of victims affected by this large-scale hack was estimated to be around 21.5 million individuals. Although the Chinese media denied of any government involvement in the hack, numerous government officials and experts have stated that the evidence demonstrated that one or another part of the Chinese government was most likely responsible for this breach of information. Judging from the magnitude and impact of this cyber attack, currently by far, China poses the greatest cyber threat to the United States and NATO Allies.

In recent years, cyber attacks on businesses around the world have resurfaced; ranging from attacks perpetrated by underground hacking organizations like Anonymous, to the state-sanctioned act of "ethically [hacking] foreign governments,"[19] as to the principles promoted by the U.S. military, hacks have varied in nature. The threat posed by these organizations, institutions, and governmental groups must be mitigated urgently.



[20]

Worldwide cyber attack statistics showing the forms of cyber attack techniques and their frequencies

[18] http://www.nato.int/strategic-concept/expertsreport.pdf
[19] https://www.sott.net/article/318656-US-military-trains-soldiers-to-ethically-hack-foreign-governments
[20] http://www.hackmageddon.com/2015/02/05/january-2015-cyber-attacks-statistics/

The main priority of NATO regarding cyber defence deals with the protection of its own networks against malicious cyber attacks.

The term 'cyber defence' was first included in NATO's political agenda at the Prague Summit of 2002. NATO's first centre regarding cyber defence was established in 2008, in accordance to its 2008 policy on cyber defence, as a response to the attacks on the Estonian government. The *Cooperative Cyber Defence Centre of Excellence (CCDCE)* was constructed in Estonia for the purposes of promoting research and adequate training to develop the cyber security industry, in an attempt to "enhance the capability, cooperation, and information sharing among NATO, NATO nations, and NATO partners in cyber defence by virtue of education, research and development, lessons learned and consultation."[21]

Since the Lisbon Summit of 2010, NATO has been working to improve its cyber defense in accordance with constantly evolving technologies and manpower. NATO's vital institution constructed to defend its cyberspace is known as the *NATO Computer Incident Response Capability Technical Centre (NCIRCTC)*. This branch organization provides "technical and legislative support services to respond to computer security incidents within NATO."[22] It has centralized and round-the-clock cyber defence support systems to ensure (1) preventive measures through bulletins, VA Teams, and software updates, (2) responsive measures through Incident and Intrusion Detection System (IDS) support and response, and (3) legislative support through forensic investigations and policy updates. Also, the organization maintains Rapid Reaction Teams that can support the protection of NATO and Allied networks. The NCIRCTC collects and processes security events everyday, which are actively followed by cyber defence experts. As of October 2013, there has been a NCIRCTC upgrade by 58 million Euros to enhance NATO's capability in protecting its cyber networks, which "[provided] state-of-the-art sensors, scanners and intelligent analytic capabilities to better prevent, detect and respond to cyber threats."[23]

At the Wales Summit in September 2014, NATO enhanced its policies on cyber defence, establishing that cyber defence should be included as one of NATO's core tasks of collective defence. Additionally, the policy also provides for cyber defence guidance, response procedures in giving assistance to Allied countries after a cyber attack, and the implementation of cyber defence into operational planning. The policy finally encourages ways to promote education, exercise, and awareness about the cyberspace, and encourages

[21] https://ccdcoe.org/
[22] https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf
[23] http://www.nato.int/nato_static/assets/pdf/pdf_2013_10/20131022_131022-MediaBackgrounder_Cyber_Defence_en.pdf

further cooperation initiatives within the industry, including those with international organizations and partner countries.[24]

The *Cyber Defence Committee (CDC)* of NATO has been the center of NATO's political governance of its cyber defence policies. In addition, the *Cyber Defence Management Board (CDMB)*, the *Consultation, Control, and Command Board (NC3)*, and the *Communications and Information (NCIA)* are working conjointly to ensure NATO cyber security. Furthermore, NATO conducts regular training and exercises, including the Annual Cyber Coalition Exercise in September and the NATO Cyber Range to integrate the element of cyber defence into the consideration of Alliances. During these events, hundreds of experts test their defence capabilities and seek improvements from their results. A Memorandum of Understanding on Cyber Defence was made between NATO and each of the 28 cyber defence authorities to exchange information regarding cyber defence and assistance to improve cyber intrusion prevention efforts and response capabilities.

NATO has also reached out to organizations such as the European Union (EU), the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), and the United Nations (UN) to work together in furthering cyber-security efforts. In February 2016, NATO and the EU conducted a Technical Arrangement on Cyber Defence, a platform for both organizations to collectively exchange cyber-defence related information and best practices, to better prevent and respond to technological issues. As the NATO Assistant Secretary General for Emerging Security Challenges, Sorin Ducaru, comments, "Together, NATO and the EU are stronger in defending against cyber-attacks. Intensified cooperation under this arrangement will allow us in a tangible way to better prevent cyber-attacks, but also our ability to predict, detect and respond to them."[25] Furthermore, NATO is reaching out to private sector industries through the NATO Industry Cyber Partnership (NICP), working together on information sharing exercises, education, and training initiatives.

[24]http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
[25] http://www.nato.int/cps/en/natohq/news_127836.htm

Looking forward, solutions should touch upon how NATO can effectively improve its defence against cyber attacks and improve its cyber defence capability targets for the ultimate purpose of security and the functioning of a safe cyber space, as developed through the NATO Defence Planning Process (NDPP).[26] Recognizing that the threats of cyberspace surpass international borders, nations must work together to resolve the immediate issues at hand.

A particular area of concern is drawn regarding issues on how to monitor the vast amount of data stored within the cyberspace. Although the United States has been able to monitor the cyberspace more effectively than other nations, organizations such as the National Security Agency (NSA) has drawn international controversy over issues of transparency, as individuals have become more concerned about their privacy rights concerning the US domestic and international spying practices revealed by whistleblower Edward Snowden. Moreover, the fragmentation of nation's individual policies regarding cyber-security on the international level is a major barrier to cooperation, and thus, there is a need for a holistic solution in which nations are be encouraged to work together as a collective body, in exchanging information and working with parties including, but not limited to, international organizations and partner countries. There is the need to improve coordination and cooperation by facilitating new alliance-wide common initiatives, talks and discussions with regards to the cyberspace, and the continuous update of innovative technologies.

Firstly, NATO can ensure the protection of information systems that provide important services by finding alternate mechanisms that can be used temporarily in place to continue the functioning of services even at a time when they are disrupted by a cyber-attack. By managing cross-dependency of services along with international cooperation, critical information can be best protected. Secondly, NATO can progress the fight against cybercrime by improving detection methods, raising public awareness, and promoting international cooperation on the issues at hand. Finally, in accordance with evolving security threats, the development of national cyber defence capabilities is essential for ongoing protection.

[26] http://www.nato.int/cps/en/natohq/topics_49202.htm

Canada, European Union

These countries have well-developed cyber security programs within their own nations and encourages the constant improvement of cyber attack prevention initiatives through the facilitation of discourse and innovation.

Turkey

Turkey supports the cyber security of all services and systems provided by public organizations using information technologies, although it maintains an aggressive stance in support of cyber warfare and offensive strategies as a means of defence. In 2012, the Turkish Armed Forces created a new defence unit for cyber security called the General Staff Warfare and Cyber Defence Command.[27]

United States of America

The United States of America has been a massive target of cyber attacks although it also possesses adequate infrastructure to initiate cyber attacks on other nations. In recent years, the United States of America has encouraged NATO to strengthen defences against Russian threat, emphasizing the importance of cyber defence to protect NATO networks over offensive initiatives.

1. What should NATO's exact role be regarding cyber defence?
2. Is NATO doing enough in the status quo to protect its allies in the cyberspace?
3. What obstacles may NATO encounter while trying to defend against cyber attacks?
4. How can NATO effectively answer a cyber attack?
5. How can NATO effectively track/attribute cyber attackers?
6. What other organizations should NATO partner with to improve discussions on cyber security?
7. How can NATO guarantee transparency while ensuring collective cyber defence?

[27] http://aa.com.tr/en/turkey/turkish-armys-new-cyber-defense-unit/283399

NATO - Cyber Defence
<http://www.nato.int/cps/en/natohq/topics_78170.htm?>

UNIDIR - Cyber Security and Cyber Warfare
<http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>

NATO Cooperative Cyber Defence Centre of Excellence
<https://ccdcoe.org/about-us.html>

NATO - Strategic Concept 2010
<http://www.nato.int/cps/en/natohq/topics_82705.htm>

NATO - NATO: Changing gear on cyber defence
<http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/>

Centre for Complex Operations - European Union and NATO Global Cyber-security Challenges: A Way Forward
<http://cco.ndu.edu/Publications/PRISM/PRISM-Volume-6-no-2/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/>

"30 Years of Risky Business: A Cybersecurity Timeline -- GCN." GCN. GCN, 03 June 2013. Web. 23 Aug. 2016.

"Active Engagement, Modern Defence - Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation Adopted by Heads of State and Government in Lisbon." NATO. NATO, 19 Nov. 2010. Web. 23 Aug. 2016.

"Anonymous' 'Hack Israel Day' Could Impact the Entire World." Recode. Recode, 2016. Web. 23 Aug. 2016.

Barnes, Julian E. "NATO Recognizes Cyberspace as New Frontier in Defense." *The Wall Street Journal.* The Wall Street Journal, 14 June 2016. Web. 23 Aug. 2016.

"Cyber Defence." *NATO Multimedia Library*. NATO, n.d. Web. 23 Aug. 2016.

"Defence Planning Process." NATO. NATO, 11 Nov. 2014. Web. 23 Aug. 2016.

"Experts Discuss Intensifying Cyber Defence Cooperation." NATO. NATO, 28 May 2010. Web. 23 Aug. 2016.

"The History of Cyber Attacks - a Timeline." NATO Review. NATO, n.d. Web. 23 Aug. 2016.

"Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired.com. Conde Nast Digital, 03 Mar. 2016. Web. 23 Aug. 2016.

"January 2015 Cyber Attacks Statistics." HACKMAGEDDON. HACKMAGEDDON, 2015. Web. 23 Aug. 2016.

"A Look at Estonia's Cyber Attack in 2007." NBC News. NBC News, 2009. Web. 23 Aug. 2016.

"NATO Cooperative Cyber Defence Centre of Excellence." NATO Cooperative Cyber Defence Centre of Excellence. CCDCOE. Web. 23 Aug. 2016.

"NATO and the European Union Enhance Cyber Defence Cooperation." NATO. NATO, 10 Feb. 2016. Web. 23 Aug. 2016.

"NATO: Changing Gear on Cyber Defence." NATO Review. NATO, n.d. Web. 23 Aug. 2016.

"US Military Trains Soldiers to 'ethically Hack' Foreign Governments" Signs of The Times. Signs of The Times, 18 May 2016. Web. 23 Aug. 2016.