

Committee: General Assembly

Topic: Cybersecurity

Country: Republic of Poland

Delegate: Vivian Chen, Heritage High School

Background:

With the rise of technology in the past two decades, cybersecurity has become a critical issue facing nations and their citizens. Governments and businesses, big and small, are now at risk of foreign attacks and the loss of trade secrets and data. Both foreign intelligence agencies and criminal hackers pose threats to national sovereignty, and violate the rights of privacy of individuals. Due to society’s growing dependence on technology, cybersecurity is vital to maintaining economic growth and the functioning of social systems (NUMUN).

Current Situation:

Poland, like many other nations, falls victim to cyber espionage, mainly from Russia and Ukraine (Riley). Within the past decade, Poland has made the growing issue of cyber security a priority, introducing legal reforms and increasing funding of fortifications (“Cybersecurity”). In 2014, the percent of total IT expenditure on cybersecurity by Polish PwC’s rose from 2.7% to 5.5%, 2% higher than the world average (“Risk”). Poland has been a long-time adversary of cyberattacks, ratifying and integrating the treaty proposed at the 2001 Budapest Convention on Cybercrime, the first of its kind that motioned to settle conflicts on cyber espionage (NUMUN). Poland recognizes and urges respect for international laws as a foundation for eliminating espionage and cyberattacks (“Cybersecurity”).

Stance/Possible Solutions

Poland emphasizes “pursuing active cyber defense, protecting and defending tele-information systems and accumulated data, and supporting key private firms in their cybersecurity efforts” as stated by Bronislaw Komorowski, former President of Poland (“Cybersecurity”). Poland strongly condemns those involved in cyber espionage, and wishes to eliminate it in order to promote cybersecurity and justice among the international community. To do this, Poland introduces the PACT plan, which stands for Partnership, Accountability, Communication, and Technology. In order to make cybersecurity attainable for all countries, developed and developing, Poland encourages the cooperation and partnership of developing countries to aid in cybersecurity efforts for undeveloped ones. Developed countries who choose to do so will be incentivized through economic means. In addition, Poland urges the United Nations with cooperation with NGOs (Microsoft, NPower, TechSoup Global, CastleCops, Center for Internet Security, etc.) to fund cybersecurity measures.

The second element of the PACT Plan, Accountability, serves to hold countries responsible for malicious actions. This includes the formation of an Espionage Court as an extension of the International Court of Justice. When countries fail to adhere to cybersecurity standards and protocol, that is, the gathering of information through secretive means intended to harm the opposing nation economically and/or politically, the perpetrators will be tried against the Espionage Court, composed of 10 judges selected by the ICJ based upon merit, and each serving a five-year term.

Furthermore, the third element of PACT, communication, highlights the power of discussion and open dialogue in fortifying cybersecurity. Poland encourages the creation of Joint Communication Centers, where countries can share their gathered information to promote transparency. Only when countries trust each other with confidential information and form a pact against cyber espionage can the cybersecurity issue be solved. In the Joint Communication Centers, countries can warn each other regarding threats from cyber criminals, terrorism, non-state organizations, etc. The Joint Communication Centers consist of two subgroups, regional and international. Regional JCCs could be composed of already existing intelligence agencies such as the Central European Cyber Security Platform-CECSP (composed of Czech Republic, Slovakia, Hungary, Austria) which Poland is a part of. The regional committees would form the overarching, international JCC.

The final component of the PACT plan, technology, addresses the implementation of fortifying cybersecurity. Through technology, preventative measures and defense systems/ software can be used to effectively combat cyber threats. In terms of technology, Poland is implementing the concepts of procedures, people, and technical software as a recipe for success towards eliminating espionage. Poland encourages the hiring, training, and providing incentives for IT personnel, and the providing and funding of advanced security/technology systems. The establishment of over watch groups such as the Computer Emergency Response Teams (CERT) and the National Competence Centre in native Poland, and all around the globe will serve to limit cyber-attacks. In addition, Poland supports the creation of international conferences on avoiding cybercrime, including the SECURE 2015 Conference, European Cybersecurity Forum-CYBERSEC.EU, and the International Conference on Cyber Security-Safety and Security beyond Borders (U.N.), those of which Poland has attended. Furthermore, Poland supports the adoption of simulations which focus on training security experts. Ones currently in practice, such as CYBEREUROPE of the European Union and NATO Locked Shields, have proved as effective exercises (U.N.). In such events, it is a developed country’s responsibility to include developing countries in their developing their cybersecurity capabilites. In order to fund the technology necessary, especially for developing nations, Poland highlights the 5.4-billion-dollar budget allocated to the General Assembly by the United Nations.

Poland has always supported democracy and fairness. Cybersecurity is a basic entitlement to countries and must be respected. Agents hindering cybersecurity such as cyber espionage must be stopped, as it is an unjust form of gathering information and likewise violates one’s national sovereignty. Poland looks forward to cooperating with other delegations to achieve cybersecurity and an equal playing field for all nations.

Works Cited

“Cybersecurity Doctrine of the Republic of Poland.” *National Security Bureau (BBN),* 22 Jan. 2015, http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html

Northwestern University Model United Nations. *Disarmament and International Security Topic A: Contemporary Espionage*. Northwestern University, 2014, http://numun.org/blog/wp-content/uploads/2014/02/DISEC-Topic-A-Contemporary-Espionage.pdf

Riley, Michael, and Jordan Robertson. “Cyberspace Becomes Second Front in Russia’s Clash with NATO.” *Bloomberg*, 15 October 2015. https://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato

 “Risk of cyber attacks on polish sme on the rise.” *Ministry of Treasury of the Republic of Poland,* 26 Jan. 2015, http://www.msp.gov.pl/en/polish-economy/economic-news/6053,Risk-of-cyber-attacks-on-polish-sme-on-the-rise.html.

U.N. General Assembly, 71st Session. *Developments in the field of information and telecommunications in the context of international security- Replies Received from Countries*, *Poland*. Supp. No. 172 (A/71/172). Official Record. New York, 2016.