SCUSA 71: RUSSIA TABLE PAPER

November 2, 2019

DECISION MEMORANDUM

FROM: SCUSA 71 Roundtable on Russia

SUBJECT: Russian Interference and Protection of U.S. Democratic Institutions

1. Purpose. This memo outlines policy recommendations for protecting American cyberspace and elections from the Russian Federation. Domestically, we recommend expanding and reorganizing existing domestic cybersecurity agencies and investing in cyber education. Abroad, we suggest negotiating an agreement to regulate cyberspace, creating a well-defined system for responding to Russian cyberattacks, and expanding NATO efforts to incorporate cybersecurity.

2. Background and Analysis. Russian interference in the 2016 Presidential Election highlighted the importance of the Russian cyberthreat as well as the vulnerability of U.S. systems. This growing problem has not escaped the notice of national security advisors.[1] Executive Order 13800, for example, emphasizes the need to repair aging U.S. technology infrastructure and assist states, local governments, and the private sector in hardening systems against attack.[2] Efforts to combat interference in the public sector have been disorganized, however. Although Congress allocated nearly $400 million in 2018 to prevent interference in the upcoming election, insufficient systems and political constraints leave us still vulnerable to Russian incursions.[3]

The U.S. Department of Defense Cyber Command has reasserted its commitment to NATO and encouraged member states to develop intelligence and cyber capabilities.[4] NATO allies have also expressed interest in developing responses to cyberattacks, especially in the context of the Russian cyberthreat.[5]

There is no broad consensus on how international law applies to the cybersphere, however. The United Nations Group of Governmental Experts on Informational Security was unable to produce a consensus report at its final meeting in 2017.[6] Although the UN has created a new

---

[1] The White House, "National Cyber Strategy," NIST, accessed November 1, 2019, https://www.nist.gov/node/1563951/edit%20National%20Cyber%20Strategy.

[2] "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Department of Homeland Security, (February 27, 2019), https://www.dhs.gov/cisa/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

[3] Elizabeth Howard, Defending Elections: *Federal Funding Needs for State Election Security*, New York: Brennan Center for Justice, (2019), https://www.brennancenter.org/our-work/research-reports/defending-elections-federal-funding-needs-state-election-security

[4] "Cyber Defence," North Atlantic Treaty Organization, (September 6, 2019) https://www.nato.int/cps/en/natohq/topics_78170.htm.

[5] Trey Herr and Jacquelyn Schneider, "Sharing is Caring: The United States' New Cyber Commitment for NATO," Council on Foreign Relations, (October 10, 2018) https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato.

[6] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?," The Diplomat, (July 31, 2017) https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

group of governmental experts, it will not convene until 2021, which will be too late to deter Russian attacks on the 2020 U.S. Presidential Election.[7]

U.S. foreign policy response to Russian cyberattacks has been to sanction individuals and organizations under Executive Orders 13694 and 13757[8]. Although sanctions alone have not prevented Russian cyberattacks, they have imposed costs on Russia for its aggressive actions. They have hurt the Russian economy, severely reduced foreign direct investment in Russia, and caused financial losses to prominent Russian businessmen.[9]

3. Recommendation. The U.S. government must provide additional funding and resources to the Cybersecurity and Infrastructure Security Agency in order to improve its defensive cyber capabilities. Increasing the agency's oversight will allow CISA to better conduct rapid and concentrated defensive operations. In particular, CISA must work with the Election Assistance Commission to provide secretaries of state in the fifty states with recommendations, tools, and standards on elections cybersecurity.

The U.S. government must also increase support of U.S. Cyber Command by expanding its span of control. A centralized cyber command for all offensive capabilities will improve our ability to apply the principles of speed and concentration.

We must support information technology and cyber education in order to build expertise. The federal government should increase the number of collegiate computer science scholarships and provide grants to states to incentivize cyber education.

The U.S. will request that NATO schedule a summit to discuss cyber deterrence, information sharing, and the purpose of Article 4 in a new era of cyber warfare. The summit should also consider NATO policy on invoking Article 5 with regard to cyber conflict so member states can respond quickly to aggression.

By July 2020, high-ranking U.S. and Russian officials must begin talks on a bilateral agreement to define and prohibit cyber interference in elections, critical infrastructure, and governmental agencies. This agreement will reinforce domestic security for the United States while providing a clear course of action in case of Russian incursion into the American cybersphere. Until an agreement is reached, the U.S. should continue to deter Russian cyber interference through economic sanctions on individuals and organizations involved in attacks.[10]

---

[7] "Group of Governmental Experts – UNODA," United Nations Office of Disarmament Affairs, Accessed (November 1, 2019): Retreived from https://www.un.org/disarmament/group-of-governmental-experts/

[8] U.S. Department of State, "Cyber Sanctions," accessed November 1, 2019, https://www.state.gov/cyber-sanctions/

[9] Nicholas Trickett, "Russia's FDI Outlook Grim, with No Chinese Rescue in Sight," *Russia Matters*, (2019) Retrieved from https://www.russiamatters.org/analysis/russias-fdi-outlook-grim-no-chinese-rescue-sight.

[10] Rennack, Dianne E., Welt, Cory. *U.S. Sanctions on Russia: An Overview* (CRS Report No. IF10779,) (2019,) Retrieved from Congressional Research Service website: https://crsreports.congress.gov/product/pdf/IF/IF10779

References

"Cyber Defence," North Atlantic Treaty Organization, (September 6, 2019): https://www.nato.int/cps/en/natohq/topics_78170.htm.

"Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Department of Homeland Security. (February 27, 2019): https://www.dhs.gov/cisa/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

"Group of Governmental Experts – UNODA," United Nations Office of Disarmament Affairs, Accessed (November 1, 2019): Retreived from https://www.un.org/disarmament/group-of-governmental-experts/

Herr, Trey and Schneider, Jacquelyn. "Sharing is Caring: The United States' New Cyber Commitment for NATO." Council on Foreign Relations. (October 10, 2018): https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato.

Howard, Elizabeth. "Defending Elections: Federal Funding Needs for State Election Security." New York: Brennan Center for Justice.(2019): https://www.brennancenter.org/our-work/research-reports/defending-elections-federal-funding-needs-state-election-security

Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?." The Diplomat. (July 31, 2017): https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Rennack, Dianne E., Welt, Cory. "U.S. Sanctions on Russia: An Overview (CRS Report No. IF10779)." (2019): Retrieved from Congressional Research Service

The White House. "National Cyber Strategy." NIST: https://www.nist.gov/node/1563951/edit%20National%20Cyber%20Strategy. https://crsreports.congress.gov/product/pdf/IF/IF10779

Trickett, Nicholas. "Russia's FDI Outlook Grim, with No Chinese Rescue in Sight." Russia Matters. (2019): Retrieved from https://www.russiamatters.org/analysis/russias-fdi-outlook-grim-no-chinese-rescue-sight.

U.S. Department of State. "Cyber Sanctions." accessed November 1, 2019. https://www.state.gov/cyber-sanctions/