Initial Post: Increasing cyber security investment in the energy industry

Cyber Security has become a global issue because it is a means of attack that can affected nations in political, financial, and physical ways. Consequently, most modern nations now include cyber as a military domain, similar to air, land, sea and space (The Economist, 2010; Leventopoulos & Benias, 2017). Despite being a recognized military domain (Constantin, 2012), cyber security investment is currently the sole responsibility of the private sector critical infrastructure owners.

Consider critical infrastructure such as energy production and transportation organizations that must be protected from nation state adversaries as well as terrorist groups and criminal organizations (Besenyő & Fehér, 2020). Cyber security investment requirements are defined by regulatory bodies for companies that produce electricity or operate pipelines (Transport Security Administration, 2021); due to the scale and specialization, control implementation is more expensive than conventional internet-based applications Booth et al. (2019). North American energy companies must operate as profitable entities, meet regulatory requirements, and participate in a public private partnership (Cybersecurity & Infrastructure Security Agency, N.D.) with the U.S government.

Although military force would be used to quell damage to life or physical property owned by the private sector (Berlin & Romore, 2020), a similar response capability is not normally available when law abiding organizations fall victim to cyber-attacks. An official statement regarding the recent ransomware attack against Colonial Pipelines mentions the company engaged a third-party cyber security firm to assist with response (Colonial Pipeline, 2021), further evidence of cyber security self-funding. The Bloomberg (2021) article on the Colonial breach reports government agencies like CISA and the U.S. Department of Energy are monitoring the issue but there is no mention of military, technical or financial support.

Although it is encouraging to see governments providing cyber security research funding (Government of Canada, 2021), the current implementation and maintenance costs may need to be partially offset through a commercial mechanism such as tax credits to increase corporate appetites for cyber security investment and the pace of implementation.

References

Berlin, J. & Romore, K. (June 1,2020) 12 times the president called in the military domestically*. Chicago Tribune.* Available from: https://www.chicagotribune.com/news/ct-national-guard-deployments-timeline-htmlstory.html [Accessed 9 May 2021]**.**

Besenyő, J. & Fehér, A. (2020) Critical Infrastructure Protection (CIP) as New Soft Targets: Private Security VS. Common Security. *JOURNAL OF SECURITY AND*

SUSTAINABILITY ISSUES 10(1): pp. 11-14. Available from: https://www.researchgate.net/publication/344467597_CRITICAL_INFRASTRUCTURE_PROTECTION_CIP_AS_NEW_SOFT_TARGETS_PRIVATE_SECURITY_VS_COMMON_SECURITY [Accessed 8 May 2021]

Booth, A., Dhingra, A., Heiligtag, S., Nayfeh, M. & Wallance, D. (2019) Critical infrastructure companies and the global cybersecurity threat. Available from: https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat [Accessed 9 May 2021].

Constantin, L. (2012) NSA chief asks hackers at Defcon for help securing cyberspace Available from: https://www.computerworld.com/article/2505115/nsa-chief-asks-hackers-at-defcon-for-help-securing-cyberspace.html [Accessed 07 May 2021].

Cybersecurity & Infrastructure Security Agency. (N.D.) Critical Infrastructure Sector Partnerships
Available from: https://www.cisa.gov/critical-infrastructure-sector-partnerships [Accessed 8 May 2021].

Government of Canada. (2021) Cyber Security Innovation Network. Available from: https://www.ic.gc.ca/eic/site/149.nsf/eng/home [Accessed 08 May 2021].

Leventopoulos, S. A. & Benias, N. (2017) Cyber Warfare Affecting Land, Sea, Air and Space Operations. *Journal of Computations & Modelling* 7(1): pp. 29-56. Available from: https://www.researchgate.net/publication/313477947_Cyber_Warfare_Affecting_Land_Sea_Air_and_Space_Operations [Accessed 07 May 2021].

The Economist. (July 1, 2010) Briefing: War in the fifth domain. *The Economist.* Available from: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain [Accessed 07 May 2021].

Transport Security Administration (2021) Resources : Pipeline Security. Available from: https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf [Accessed 9 May 2021].