Q&A

Walter Miron

Q. Should the Internet be considered critical infrastructure?

A. In discussing critical infrastructure, Vespignani (2010) put forth the Internet as a "classic example". However, this view is not widely shared. Given its relatively young age, its ongoing amplification, its increasing complexity, and our growing dependence on it, viewing the Internet as a "classic" anything overlooks our need to improve, adapt to, and secure the Internet of the future. Furthermore, even though "information technology" is typically recognized as critical infrastructure, the Internet deserves particular attention as a delivery vehicle for essential services whose disruption holds the potential for societal and financial impacts. Here, I will argue that the Internet should indeed be considered critical infrastructure and that this view will bring benefits in securing it as a delivery vehicle for essential services whose interdependence amplifies the potential impacts of disruptions resulting from failures, natural disasters, and cyber-attacks.

Critical infrastructure is defined as resources that are considered essential to maintaining society, the disruption of which has wide impact on society and the economy (Murray & Grubesic, 2012; Singh et al., 2014; Yusta et al., 2011). Researchers and governments have classified 13 sectors as critical infrastructures, including the general category of "information technology" along with the food supply, banking and finance, telecommunications, defense, emergency services, energy, healthcare, national monuments, shipping, transportation, and water distribution (Singh et al., 2014). In India, however, Internet infrastructure and access is considered one of the critical infrastructure categories (Singh et al., 2014).

Where a failure in one system leads to a failure in another system, these critical infrastructures are said to be interdependent (Vespignani, 2010). Interdependent networks are thought to be fragile compared to an isolated system (Buldyrev et al., 2010; Vespignani, 2010), and the complexity introduced through this interdependency presents design and security challenges (Xiao-Juan & Li-Zhen, 2010). Modern critical infrastructures rely on information and communications technology (ICT) for their control. Rahman and colleagues (2011) define this reliance on ICT as cyber-interdependency and report that data communications account for 85% of failures in cyber-interdependent systems.

Considering the proliferation of high-speed fixed and mobile broadband networks, the delivery of essential services, and the cyber-interdependence that this scenario creates, it can be argued that the Internet has become critical infrastructure. Moreover, considering the Internet as critical infrastructure may help us confront the many challenges relating to the Internet's current design, its regulatory environment, and its cybersecurity assessment practices. In the sections that follow, this argument will be expanded. First, I will consider the amplification of the Internet and its transformation into a critical ICT infrastructure through its use as a delivery vehicle for essential services. Next, I will present definitions of critical infrastructure and cyber-interdependence and compare these definitions to the modern Internet. Finally, I will highlight the need for design practices and frameworks for assessment that may serve to improve the reliability and security of the Internet.

The Internet as a Delivery Vehicle for Essential Services

Essential services such as telephony, broadcast services, online banking and trading, and transportation systems for cross-border trade are increasingly dependent on the reliable and secure operation of the Internet. Simply put, modern communications networks, including the Internet, are critical infrastructures because they deliver essential services (Cetinkaya et al., 2011).

Phahlamohlaka and colleagues (2011) report that, since 2006, the critical national infrastructure in the United States has become increasingly dependent on the Internet. They go on to state that, “The United States economy and government are the most dependent in the world on the Internet.” Consider telephony services: recently, Network World reported that 79% of landline voice customers will switch to other alternatives for voice services such as mobile and Internet phones, and that 47% are already using voice-over-IP products (Hettick, 2014).

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

In the financial market, roughly a third of respondents 18 to 44 years of age reported that they used mobile Internet services to conduct banking transactions (U.S. Federal Reserve, 2012). The online payment market transaction volume through Square credit card readers (square.com) has been doubling annually from 2009 to 2013 (Olson, 2014). Delivering financial services over the Internet is another indicator that the Internet is a critical infrastructure.

Transportation and cross-border trade over the Canada–U.S. border contributes 1.8 billion US dollars a day to the economies of both nations with disruptions having major financial impacts (Von Hlatky & Trisko, 2012). Cross-border security has tightened since the September 11th attacks on New York City and the Washington DC metropolitan area, hindering border transit and effectively creating a non-tariff barrier to trade (Von Hlatky & Trisko, 2012). To reduce the impacts to the transportation of goods across this international border, Canada and the United States have launched the Free and Secure Trade (FAST) program that allows low-risk carriers, drivers, and importers expedited border transit (CBSA, 2013). The FAST program allows clearance transactions, applications, and approvals to be conducted online, and implements radio-frequency identification (RFID) technology to minimize delays at border crossings. The use of technology aids in removing non-tariff trade barriers imposed on the transportation of goods and people with heightened security in the post-911 era (Von Hlatky & Trisko, 2012).

The disruption of any of these essential services such as telephony, broadcast services, online banking and trading, and transportation systems for cross-border trade holds the potential for significant impacts to the economy and communications and illustrates that the unintended consequence of the Internet as the great equalizer of innovation leads it to become critical infrastructure by definition due to its cyber-interdependence with the services that it now provides. However, despite this importance, neither regulators nor industry has defined Internet delivery mechanisms in this way nor developed guidelines for improving reliability or security of these assets.

Interdependence of the Internet and Critical Infrastructure

Poljansek and colleagues (2012) consider water, energy, and communications systems as "lifeline utility systems", assigning them special significance due to their interdependence. Disruptions in one part of the network can cause cascading impacts on other parts of the network due to increased traffic of re-routing and other factors (Poljansek et al., 2012; Yusta et al., 2011). Information technology and telecommunications rely on energy, and all other sectors rely on them. Therefore, any disruption to these sectors can lead to adverse impacts to other sectors, (Chapman et al., 2013; Singh et al., 2014). Moreover, critical infrastructures such as public safety and emergency medical services, banking and finance, postal and shipping, healthcare, agriculture and food, transportation, and manufacturing rely heavily on ICT for control and decision making. This cyber-interdependency makes these infrastructures susceptible to ICT failures (Rahman et al., 2011; Singh et al., 2014).

These cyber-interdependencies form a critical situation for Internet delivery of essential services, and infrastructures must be designed, built, and assessed appropriately. However, whereas underlying infrastructure such as electricity or telecommunications are considered to be critical infrastructures, assets deployed in delivering Internet services are not. This discrepancy leads to a situation where, what were once independent essential services delivered to customers on tailored infrastructure elements, may now be delivered together over the Internet without regulatory or industry focus on reliability and security.

Threats to critical infrastructure come in the form of equipment failures, natural disasters, and cyber-attacks. As Vespignani (2010) states, "the most dangerous vulnerability is hiding in the many interdependencies across different infrastructures". When contemplating failures, "near-worst-case scenarios can be as devastating as worst-case scenarios" (Murray & Grubesic 2012).

Independent networks of infrastructure are more fragile than each network in isolation; they fail more abruptly, and at a point of lesser-sustained damage than would an isolated network (Buldyrev et al., 2010). Interdependence of the networks means that "localized damage in one system may lead to a failure in another, triggering cascading and escalating failures" (Vespignani, 2010). This situation further emphasizes the risk to the Internet given its role as a data communications network. One such example of this risk of a cascading event is the Italian power failure of 2003, where power failures impacted communications and the Internet, which in turn further impacted power stations (Buldyrev et al., 2010). Human factors are another key source of failures. Of all critical infrastructure disruptions, 85% are attributable to the failure of data commu-

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

nications networks (Rahman et al., 2011), and human-related failures account for 50% of Internet disruptions (Cetinkaya et al., 2011).

Infrastructures are dependent on and impacted by the environments in which they operate, making them susceptible to natural disasters (Poljansek et al., 2012). Water, transportation, fuel, and power are coupled together (Buldyrev et al., 2010), and failures in any of these domains will have cascading affects on other domains. Hurricanes Katarina and Andrew in the United States and the Fukijama Earthquake in Japan are examples of the impact of the environment on critical infrastructures.

However, not all human failures originate from errors. Cyber-attacks are on the rise, and our increasing connectedness, data, and flows provide more opportunities for exploitations by actors with malicious intent (Dupont, 2013). Due to their interdependency, energy, information technology, and telecommunications are the main cascade-initiating sectors and therefore are primary targets for malicious attacks (Singh et al., 2014). Recent military actions in Georgia and Estonia were coordinated with attacks on Internet resources and were aimed at impacting interdependent critical infrastructure in the financial, industrial, and control infrastructures (Phahlamohlaka et al., 2011).

The increase in both volume and sophistication of cyber-attacks as well as the increase in natural disasters supports a call for the development of guidelines for building and assessing reliability and security readiness of Internet assets. Next, I will discuss steps that can be taken to address the risk of failure of essential services due to disruptions of the Internet.

Recognizing the Internet as Critical Infrastructure

The interdependency between critical infrastructure elements is a key factor in effectively securing them (Xiao-Juan, & Li-Zhen, 2010). Thus, our growing dependency on ICT corresponds with the increasing importance of protection designs for critical infrastructures (Merabti et al., 2011). Therefore designing for resiliency is important because networks cannot be built for true 100% availability (Cetinkaya et al., 2011). These designs for critical infrastructure protection should include diversification, separation, avoidance, and hardening strategies (Murray & Grubesic, 2012). However, significant investments of human and financial resources are required to fortify critical infrastructure, including the Internet (Cetinkaya et al., 2011; Murray & Grubesic, 2012).

Regulators and academics have expressed interest in protecting critical infrastructure (Poljansek et al., 2012); however, this interest has not led to frameworks prescribing action to treat the Internet as critical infrastructure. Current initiatives at federal, sub-federal, and local levels lack methodological frameworks for evaluating infrastructure protection (Murray & Grubesic, 2012), and with cyber-capabilities outpacing methodologies and legal frameworks for operational control (Phahlamohlaka et al., 2011), priority must be placed on protecting these critical infrastructures by state and federal governments (Singh et al., 2014). Given that Internet access and assets are primarily owned and operated privately, cooperation between the owners and government agencies is required, along with regulatory oversight (Murray & Grubesic, 2012).

Conclusion

To successfully rise to the challenges of building and securing reliable cyber-interdependent networks for the delivery of services such as Internet telephony, online banking, trading, and payment processing , I argue that we must consider the Internet as critical infrastructure. To complement this view, I recommend the development and adoption of a framework for designing in security and reliability and assessing the readiness of interdependent networks of critical infrastructure.

Reliability and security of networks on the scale of the Internet require significant investments of time, resources, and funding. Owing to the private ownership of most Internet delivery resources, and the competition in the Internet access market and the services delivered over it, public and private cooperation is required in defining and implementing a framework for the construction, security, and assessment of these critical infrastructures and key resources. In addition to the regulatory oversight needed to ensure reliable and secure operation of these key resources, business models are needed that recognizes the value of reliability and security in the delivery of essential services over the Internet.

Considering the maturation of the Internet into a delivery vehicle for essential communications and financial, trading, and broadcast services, the complexities of designing reliable and secure interdependent networks of critical infrastructure, and the increase in the volume and sophistication of cyber-attacks as well as natural

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

disasters, the Internet must become broadly recognized as critical infrastructure. To do so would represent an opportunity for the industry, researchers, and regulators to cooperate to ensure the reliable and secure operation of the future Internet.

About the Author

Walter Miron is a Director of Technology Strategy at TELUS Communications, where he is responsible for the evolution of their packet and optical networks. He has over 20 years of experience in enterprise and service provider networking conducting technology selection and service development projects. Walter is a member of the research program committee of the SAVI project, the Heavy Reading Global Ethernet Executive Council, and the ATOPs SDN/nFV Working Group. He is also the Chair of the Venus Cybersecurity Corporation and is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada.

References

Buldyrev, S., Shlomo, H., Roni, P., Gerald, P., & Eugene, S. 2010. Catastrophic Cascade of Failures in Interdependent Networks. *Nature,* 464(7291): 1025–1028. http://dx.doi.org/10.1038/nature08932

CBSA. 2013. Free and Secure Trade (FAST). *Canadian Border Services Agency.* Accessed January 10, 2015: http://www.cbsa-asfc.gc.ca/prog/fast-expres/menu-eng.html

Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. 2013. Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach. *Telecommunication Systems,* 52(2): 751–766. http://dx.doi.org/10.1007/s11235-011-9575-4

Chapman, L., Azevedo, J. A., & Prieto-Lopez, T. 2013. Urban Heat & Critical Infrastructure Networks: A Viewpoint. *Urban Climate,* 3: 7–12. http://dx.doi.org/10.1016/j.uclim.2013.04.001

Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review,* 3(7): 6–11. http://timreview.ca/article/700

Hettick, L. 2014. Surveys Point to Increased Adoption of VoIP and Wireless Substitution. *Network World.* Accessed January 10, 2015: http://www.networkworld.com/article/2455174/

Merabti, M., Kennedy, M., & Hurst, W. 2011. Critical Infrastructure Protection: A 21st Century Challenge. In *Proceedings of the International Conference on Communications and Information Technology (ICCIT 2011):* 1–6. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICCITECHNOL.2011.5762681

Murray, A. T., & Grubesic, T. H. 2012. Critical Infrastructure Protection: The Vulnerability Conundrum. *Telematics and Informatics,* 29(1): 56–65. http://dx.doi.org/10.1016/j.tele.2011.05.001

Olson, P. 2014. Square Strikes Nationwide Payment Deal With Whole Foods. *Forbes.* Accessed January 10, 2015: http://www.forbes.com/sites/parmyolson/2014/02/11/square-strikes-nationwide-payment-deal-with-whole-foods/

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. 2011. Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cyber Security Policy Implementation. In *Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW 2011):* 1–14. Laxenburg, Austria: International Federation for Information Processing. http://hdl.handle.net/10204/5162

Poljanšek, K., Bono, F., & Gutiérrez, E. 2012. Seismic Risk Assessment of Interdependent Critical Infrastructure Systems: The Case of European Gas and Electricity Networks. *Earthquake Engineering & Structural Dynamics,* 41(1): 61–79. http://dx.doi.org/10.1002/eqe.1118

Rahman, H. A., Martí, J. R., & Srivastava, K. D. 2011. A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures,* 7(4): 265–288. http://dx.doi.org/10.1504/IJCIS.2011.045056

Singh, A. N., Gupta, M. P., & Ojha, A. 2014. Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario. *International Journal of Critical Infrastructure Protection,* 7(2): 71–85. http://dx.doi.org/10.1016/j.ijcip.2014.04.003

U.S. Federal Reserve. 2012. FRB: Current Use of Mobile Banking and Payments. *Board of Governors of the Federal Reserve System.* Accessed January 10, 2015: http://www.federalreserve.gov/econresdata/mobile-devices/2012-current-use-mobile-banking-payments.htm

Vespignani, A. 2010. Complex Networks: The Fragility of Interdependency. *Nature,* 464(7291): 984–985. http://dx.doi.org/10.1038/464984a

Von Hlatky, S., & Trisko, J. N. 2012. Sharing the Burden of the Border: Layered Security Co-operation and the Canada–US Frontier. *Canadian Journal of Political Science,* 45(1): 63–88. http://dx.doi.org/10.1017/S0008423911000928

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and Interdependency of Critical Infrastructure: A Review. In *Proceedings of the Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA 2010):* 1–5. Washington, DC: IEEE. http://dx.doi.org/10.1109/INFRA.2010.5679237

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. 2011. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art. *Energy Policy,* 39(10): 6100–6119. http://dx.doi.org/10.1016/j.enpol.2011.07.010

Citation: Miron, W. 2015. Q&A. Should the Internet Be Considered Critical Infrastructure? *Technology Innovation Management Review,* 5(1): 37–40. http://timreview.ca/article/865

Keywords: cybersecurity, Internet, critical infrastructure, cyber-attacks, vulnerabilities, information technology, communication networks