Canadian Journal of Law and Technology

Volume 19 | Number 1 Article 9

1-31-2023

Perceiving Critical Infrastructure with A New Awareness of Cyber Risk

Duncad Card

Perceiving Critical Infrastructure with A New Awareness of Cyber Risk

Duncan Card[*]

North America's critical infrastructure has been the subject of cyber-attack, in various cycles of activity, for many years. In March of 2017, a cyber-attack caused periodic "blind-spots" for electricity distribution grid operators in the Western US for about 10 dangerous hours. In May of this year, there was panic at the gas pumps across many States in southeastern United States, which has been attributed to a cyber-attack on a major US pipeline that disrupted fuel supplies to the US East coast. US Commerce Secretary Raimondo soon after that attack announced that those sorts of attacks are becoming more frequent and that combating such attacks against critical infrastructure is a "top priority" of the Biden Administration. At home, the Canadian Center for Cyber Security's 2020 Report on "National Cyber Threat Assessment" warned that foreign provocateurs "are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure." On March 11, 2021, the Trade Commissioner Service of Canada stated, in its report "Spotlight on Cybersecurity," that "Attacks on critical infrastructure have become a growing cause of concern for governments and provide sector providers around the world. . .the increase of inter-facing networks has led to an increase in the number of cyber-attacks (on those) infrastructures."

When I consider the rapidly increasing incidents of successful cyber-attack that are being perpetrated on our critical infrastructure, I can't help but wonder why such important parts of our economy, and even our national security, have remained vulnerable. In that reflection I am reminded of Albert Einstein's maxim, "The level of awareness to solve a problem is greater than the level of awareness that created the problem."

I am certainly not espousing anything radical when I repeat the traditional refrain that all critical infrastructure, whether power generation, financial systems, transportation, or parts of our critical infrastructure, are now all inherently and inextricably dependent on technology. However, too many of us do not seem to be aware that the fundamental identity of much of our critical infrastructure has now evolved far beyond that truism. We all must now be aware, as matters of corporate governance, business continuity and national security, that our critical infrastructure is no longer merely operated by computers.

No longer do computers, and other data management systems, merely sit on desks, operate inside buildings, or can be perceived of as equipment that makes other things work. The perception that technology operates, or even helps to

[*] Duncan Card, B.A., LL.P., LL.M., ICD.D; Partner, Technology Transactions, Bennett Jones LLP.

operate, critical infrastructure is now a dangerous anachronism. We all know there is a tipping point where so many industrial things have transformed into the realm of digital manifestation. Today, our critical infrastructure primarily exists as a complex agglomeration of highly-integrated, networked, distributed, interoperable, and intelligent technologies and systems that exist across many geographies, in clouds, across inter-related networks and within multifaceted digital systems. For some time now the operational essence of much of our critical infrastructure has no longer existed in the realm of industrial operation that is aided by computers. Indeed, the inherent nature and existence of our critical infrastructure has primarily transformed into a digital manifestation. The very nature and identity of our critical infrastructure must now be perceived of very differently. In the same way: advanced fighter or passenger jets can no longer be thought of as planes that fly with the aid of computers; no longer can our highly complex urban rail transportation system be merely thought of as trains that operate with the aid of computers; and, battleships can no longer be thought of a boats that merely rely on computers for their operation. Is a fully automated car, which drives unaided by a person at the steering wheel, still just a car with computers inside? Similarly, no longer can nuclear power stations, oil and gas pipelines or intelligent hospitals be thought of merely as industrial facilities that are operated with the assistance of computers. For so much of our critical infrastructure, that digital identity tipping point has been reached and surpassed. We must now all be mindful that the very being of our critical infrastructure has entered the realm of digital existence. All of the foregoing examples of critical infrastructure are the very computers that we used to think operated them. All of those examples of infrastructure, and others to soon follow, must now be perceived of as: computers that we fly; the computers with doors and wheels we get into to drive us places; digital weapons systems that float; computers that look like trains (some without wheels any more) that we sit in to commute to work every morning; computers that generate power; and, computers that allow surgery to be conducted, and patients to recover, inside them. Today's intelligent infrastructure has created a world where we must appreciate that such critical infrastructure ***is*** the computer.

The governance and commercial implications of the radical transformation in the way that we perceive of, and understand, the very identity of much of our critical infrastructure, are vast. As digitally manifest, critical infrastructure must inherently be understood as a service (now appreciated as IaaS) instead of as industrial equipment merely aided by computers. As a digital manifestation, not only does so much of our critical infrastructure more rapidly evolve and transform as a function of technological innovation, but it also evolves rapidly through the holistic integration, complete convergence and consolidated emergence of many diverse technologies, products and services. Indeed, we must now be aware that all critical infrastructure will increasingly become inextricably inter-connected and dependent upon each other for their digital operation. Therefore, with that level of awareness, we can much better understand, appreciate and respond to the risks associated with cyber security. We must now design, create, finance and manage much of our critical infrastructure primarily as highly integrated IT systems and networks, and not as the physical industrial infrastructure they are now, too often wrongly, perceived to be.

Such digital convergence and integration have profound legal, commercial, corporate governance and national security implications. Never before has so much of our critical infrastructure been digitally manifest and integrated, while simultaneously being so very exposing to malicious access and interference by those who can reach into that critical infrastructure through the very digital ramparts and corridors that provide our critical infrastructure with its digital existence. Never has the corporate governance and operational management of our critical infrastructure, and the way we perceive it to exist, had such profound national security implications. In a new appreciation for the true identity of our critical infrastructure, we may expect technology enterprises to assume leadership as the most appropriate prime contractors to build advanced transportation systems, intelligent hospitals, or even nuclear facilities. Perhaps the design, building, operation and governance of critical infrastructure will be led by technology enterprises that best understand the foundational and essential digital qualities of those facilities' vital competitive advantages, which have catalytically transformed historically industrial infrastructure into digital services. If that is the case, then the law clearly needs to catch up to the digital design, creation and operational implications of those intelligent facilities. At what point will the importance of the highly specialized digital architecture of such critical infrastructure supersede the physical architecture of the buildings? At what point will commercial technology lawyers assume the same role they do in the development of all other technology goods and services, as they should assume in the development of critical infrastructure? At what point will the corporate governance and management of critical infrastructure assume the same best practices and professional qualities of oversight that other complex digital enterprises now embrace? Would it surprise any of us if the contracts and advanced service arrangements that are negotiated and settled to develop and build next generation battleships far more closely resemble highly complex IT enterprise development and technology integration projects than they do any kind of traditional boat design and construction contract?

All aspects of our life and society are now undergoing disruptive transformation that is both driven and enabled by highly complex, innovative and integrated technology solutions that require the convergence of many complex digital systems. Our critical infrastructure is no different. If we stand any chance of designing, building, operating and managing critical infrastructure to successfully address the risk of cyber-attack and interference, we must now perceive, and be acutely aware, that our critical infrastructure is digitally (not industrially) manifest and that it correspondingly requires a quality of technological, management and governance attention that is consistent with its digital manifestation. The foreign and domestic cyber threats to our critical infrastructure are far too real, urgent and potentially devastating to our society, including to our national security, for us not to be acutely aware of the true digital identity of our critical infrastructure. Our legal, regulatory, diplomatic, corporate governance and technological response to such threats will depend upon our appreciation and awareness that. . . the infrastructure is the computer.