Cybersecurity and Safety in the 5G-Enabled Smart-Everything World

By Marin Ivezic

Marin Ivezic is a Cybersecurity & Privacy Partner in PwC Canada focused on risks of emerging technologies. He leads PwC's global 5G cybersecurity efforts as well as industrial, IoT and critical infrastructure cybersecurity services in the region.Marin worked with critical infrastructure protection organizations in a dozen countries, 20+ of the top 100 telecom companies, and a number of technology companies on understanding the geopolitics of 5G; uncovering as-yet-unknown security and privacy risks of 5G, AI and IoT; and defining novel security and privacy approaches to address emerging technology risks.

Neil Harbisson calls himself a cyborg. Without the antenna implanted in his skull, he would not be able to see colour of any kind. Born with achromatopsia, a condition of total colour blindness that affects 1 in every 30 000 people, Harbisson's physical faculties are augmented by cyber technology to grant him access to a life of greater meaning and satisfaction.

As technological evolution leads to concomitant advances in medical science, we are seeing more and more examples of humans who are integrating devices and sensors into their biological makeup.

For some, like those part of the growing "transhumanist" movement, this is a means of artistic expression or exploration of human potential. For others, it is a solution to a medical problem. Either way, it represents the most vivid and personal example of what may be called a cyber-physical system (CPS).

Harbisson campaigns for greater debate around the identity and rights of people with tech-adapted bodies. As in any discussion of CPSs, however, a more urgent part of the conversation should be security.

> Greater, more widespread risk is found in the cyber-physical systems that will soon be ubiquitous, crucial to the successful operation of industry and society.

In March 2019, an alert from the US Department of Homeland Security and the FDA warned medical professionals and patients that a broad range of implanted devices, such as defibrillators and heart monitors, were vulnerable to hacking that could cause product malfunction.

White-hackers had proven these concerns before, but the DHS announcement was chilling confirmation of the threats to human life that accompany the convergence of the cyber and the physical.

Of course, these dangers are not only seen at the level of the private individual. Greater, more widespread risk is found in the cyber-physical systems that will soon be ubiquitous, crucial to the successful operation of industry and society. Adoption of these networks is being driven by access to the internet of things (IoT) or, more accurately in cases of biological integration, the internet of everything (IoE), and is about to be accelerated with the rollout of 5G. Unfortunately, however, so are the risks.

What Is A Cyber-Physical System?

CPS is a broad, umbrella term for technologies that connect our physical world with the cyber world. It describes situations in which we find a fundamental intersection of computation, communications and physical processes without suggesting any particular implementation or application.

In addition to IoT, the cyber-physical systems term also includes Industrial Control Systems (ICS) – those setups that manage large-scale civil and industrial operations such as smart factories, water supply and power production and distribution, as well as technologies such as the Industrial Internet of Things (IIoT), robotics, drones, connected and autonomous transportation, building management systems, connected environmental controls and a myriad of other things. In essence, these are software-enabled collections of sensors, processors, and control components that automate entire, or large parts of, human operations. And they are already all around us.

> The absence of regulatory protocols leaves a huge gap as the vast majority of IoT devices are delivered without baked-in security.

Definitions of CPSs vary and many are excellent, but one that is particularly relevant to the topic is a definition I coined for the Cyber-Physical Systems Security Institute (CPSSI) in 1998: “Cyber-physical systems are physical or biological systems with an embedded computational core in which a cyberattack could adversely affect physical space, potentially impacting well-being, lives or the environment.” This definition goes beyond a technical assessment of a system’s makeup to recognize its potential impact on the world around that system. It identifies the inherent threat of cyberattacks and the dangers they inevitably pose to human life.

What Could Go Wrong?

The common appreciation of threats innate to cyber-physical systems is evolving more slowly than the technology within those systems, and more slowly than the thinking of those who wish to use this technology to cause harm.

The installed base of Internet of Things (IoT) connected devices currently stands around 30 billion, but is expected to grow to 75.44 billion worldwide by 2025, generating 79.4 zettabytes of data, according to IDC (That’s almost four times the amount of data that’s been created in history).

The use of these devices in our personal lives – everything from smart phones to smart appliances in smart homes – is already taken for granted in developed nations. Though private individuals are becoming savvier about their exposure to uninvited surveillance through these devices, most concerns are still centered around privacy and data security. Few people consider the possibility of technological tools and their components being captured for employment against them in tactile ways.

The case of vulnerable heart equipment shared earlier offers one example of how a cyber-physical attack could be lethal to individuals. Hackers have already proved that it is possible to hijack a moving vehicle remotely, raising obvious safety concerns for the driver, but also fellow drivers on the road. Now, imagine that same concern extrapolated across a network of self-driving vehicles all travelling at high speed – a scenario which, as we’ll see shortly, becomes a reality with the introduction of 5G.

This growing number of devices and their management applications connected to the IoT represents an exponentially expanding “attack surface” available to hackers and cyber-terrorists.

Unfortunately, regulations governing security of these devices and applications are underdeveloped, non-uniform and difficult to enforce across borders, an especially pertinent issue when equipment components are produced in one region, assembled in another and then sold in a third or more. The absence of these regulatory protocols leaves a huge gap as the vast majority of IoT devices are delivered without baked-in security. Even when companies do aim to make their products secure, these endeavors are usually hampered by a lack of expertise and constant pressure to be first-to-market.

This all translates into a perfect storm of cyber-physical threats in the private and social spheres, but greater dangers extend to a national, even international, level where the scale of impact is highest.

Nation-state attacks against cyber-physical systems are becoming routine. The Stuxnet malware incursion used to disrupt uranium enrichment in the Iranian plant at Natanz in 2010 saw the birth of cyber-kinetic weaponry. Since then, similar attacks have been numerous, with targets including military, civil and industrial operations.

In 2013, hackers thought to be working for a nation-state gained control of a small dam in the US, giving them the power to release water onto the communities below (had the sluice gates not been manually disabled).

The Dragonfly/Crouching Yeti espionage campaigns, thought to have taken place from 2011 to 2014, were attacks on targets in the aviation and defense industries in the US and Canada, as well as various energy industry targets in the US, Spain, France, Italy, Germany, Turkey and Poland. Similar tactics could be seen in the Ukraine in 2015, with the BlackEnergy malware causing significant power outages.

In 2017, the US electricity grid was attacked, emphasizing what experts have known for decades: critical systems such as national energy are constantly vulnerable to breach, with potentially devastating consequences for hospitals and clinics, industry, transport and civil supply services.

The Center for Strategic and International Studies (CSIS) regularly updates its list of significant cyber incidents, with a focus on cyber attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars. More than 20 such major events have been recorded in the last two months alone, with most of those attacks having an impact on cyber-physical systems. Until 2017, I used to track cyber-kinetic incidents –

those that have caused impacts in the real, physical world. I stopped because the number of such attacks increased beyond my capacity to track.

The attack surface is growing. We are already seeing a post-COVID-19 drive toward greater automation of manufacturing operations and supply chains as businesses try to mitigate the risk of reliance on human labour. These developments rely on the creation of CPSs that require increasingly sophisticated cybersecurity.

Most of these CPSs are built with 5G in mind. This budding technology is set to revolutionize industry and society, facilitating the establishment of highly integrated and largely autonomous production and distribution systems. But 5G is a two-sided coin. With its tremendous potential comes tremendous risk.

When Cyber Becomes Physical: Securing the 5G Bridge

5G has been discussed extensively in almost every industry. It is in its infancy, already showing impressive results, but yet to see widespread availability. It is set to redefine the possibilities of CPSs as well as the security requirements of those systems. But the questions linking 5G and CPSs go back some time.

On one side of the coin, the concerns. As far back as 2012, US Defense Secretary Leon Panetta warned the Business Executives for National Security of the dangers of attacks on national systems: “The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks.

“The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.”

> For the first time, smart cities will be genuinely possible: all aspects of our lives – personal, professional, social – connected in a continuous stream of data creation and interpretation.

The term “cyber Pearl Harbor” was originally credited to Richard A. Clarke, former US national coordinator for counterterrorism, in 2002. But it was even further back that another Clarke clearly saw the other side of the 5G coin: cyber-physical systems that could transcend time and space.

In 1968, Stanley Kubrick invited writer Arthur C. Clarke to collaborate in the creation of the groundbreaking epic, *2001: A Space Odyssey*. The film launched Clarke to the status of pop culture icon and indisputable futurist, though his uniquely prescient abilities were already well-established by then.

Of the many predictions Clarke made in his career, perhaps the most well-known was this one from 1964, in which the author declares: "I'm perfectly serious when I suggest that one day we may have brain surgeons in Edinburgh operating on patients in New Zealand."

As it turned out, the surgeon and the patient were both in China. The world's first remote brain surgery was performed last year by Dr. Ling Zhipei, who conducted the operation by manipulating instruments in Beijing from his location in Sanya City, 3000 kilometers away.

Though this historic event had been expected for some time, the fact that Clarke predicted it more than 55 years ago is astonishing. What's even more impressive, though, is the detail of the writer's foresight. Not only did he see remote surgery coming, but he also saw the complications that would hamper its success. In his 1975 novel, *Imperial Earth*, Clarke addresses the problem of an even slightly laggy network: "'Hawaii's almost exactly on the other side of the world – which means you have to work through two comsats in series. During tele-surgery, that extra time delay can be critical.' So even on Earth, thought Duncan, the slowness of radio waves can be a problem. A half-second lag would not matter in conversation; but between a surgeon's hand and eye, it might be fatal."

Though he wouldn't have known it then, what the writer had identified was one of the key distinctions between 4G and 5G networks.

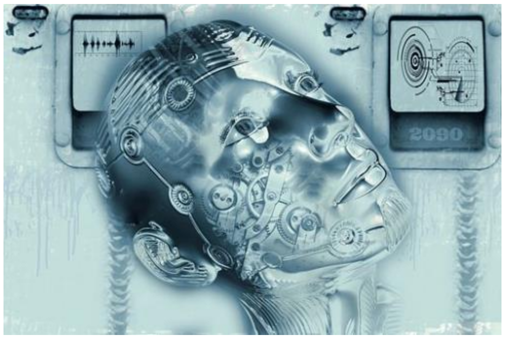
To take nothing away from Dr Zhipei's skills as a surgeon, his pioneering achievement would not have been possible without the computer, powered by a 5G network. 5G eliminates the lag and remote-control delay typical on 4G networks. But, that is not simply because it is an upgraded version of 4G. 5G is something entirely new. It is a momentous leap in potential. It has made science fiction science fact.

Though many rub their hands in glee at the prospect of super-fast movie downloads and instantly responsive gaming, the most notable impact of this technology will be through the CPSs it facilitates. It is there that we will see technology finally having the enduring societal impact it has promised for so long. But the halcyon image of humans living carefree in a hyperconnected world is also misguided.

When systems are cyber-kinetic, high speed, high efficiency, AI-driven decision making and systems autonomy are great when things are running well. But when they aren't, people can get hurt. Or worse.

A New Age of Cyber…

Another soothsayer of sci-fi is William Gibson, venerated author of Neuromancer, coiner of the term, “cyberspace” and regarded by many as a prophet of the digital age. In a recent Financial Times interview, Gibson states, “The online/offline distinction is going to be fully generational soon. Only old people will think of being on or off.”



The digital mystic is expressing a recurring theme that underpins the evangelical spirit of Neil Harbisson and other proponents of the Singularity – human and machine are moving closer and closer to becoming one. Though we are not yet at the stage of full cyber-bio assimilation, the functional integration of technology into our daily lives is already widely apparent through the IoT.

Thanks to consistently cheaper computer chips and the ubiquity of wireless networks, the IoT is expanding unabated. In a 5G world, the IoT will grow exponentially to a massive internet of things (mIoT) that includes sub-domains such as the industrial internet of things (IIoT) and critical internet of things (cIoT). The connection capacity of 5G networks will be breathtaking. For the first time, smart cities will be genuinely possible: all aspects of our lives – personal, professional, social – connected in a continuous stream of data creation and interpretation.

Our homes will be “intuitively” responsive to our every whim and taste, our offices will maximize energy efficiency and convenience, our social services will be preemptive and evolutionary.

Fleets of autonomous vehicles directed by self-managed and self-optimizing traffic control systems, public surveillance interfaces capable of refined facial recognition, civil management operations ensuring that water, energy and waste processes run increasingly smoothly – these are the anticipated fruits of a 5G world.

In return for greater convenience we are increasingly losing the control over the related cyber risks.

There are a couple of reasons for this. First, 5G is fast. Lightning fast. Its theoretical top speed (20 Gbps) is up to 200 times faster than 4G. 5G’s speed is what makes it possible to download Ultra HD movies in a matter of seconds.

Second, 5G operates with unbelievably low latency (the time it takes for a system to receive a response to a request). The average human reaction time to a stimulus is 250 milliseconds (ms). Most humans perceive 100ms as instantaneous. 5G's reaction time is between 1 and 2ms. 5G's super-low latency is what makes real-time instant gaming, remote surgery and driverless cars a reality.

5G is able to produce these sensational results because it is not like anything that has come before. Though the term "5G" is an abbreviation of "5th Generation," this nomenclature is deceiving. It suggests that 5G is simply an advanced form of 4G, just as 4G was a step up from 3G.

This is not the case.

Unlike previous generations, 5G is not a physical network. It is an all-software cloud-based configuration operated through distributed digital routers. It is a decentralized system that optimizes processing speed and power by relocating operations to the fringe.

Resting in the digital ether, built on software and managed largely by AI, 5G represents the first widespread transcendence of physical computing and communication. Perhaps ironically, then, it is in the physical realm where 5G's greatest dangers lie. Though the technology itself is agnostic, it does invite us to marry our physical lives with the cyber realm, and for all the promises in that union, there are many threats too.

...Needs A New Age of Security

There is little doubt that cyber-physical technologies are encroaching into every aspect of our lives and are evolving toward higher degrees of autonomy and adaptability.

With the explosion of CPSs connected through the upcoming 5G with its distributed structure, incredible speed and negligible latency, the reality is starting not only to match, but to exceed, the expectations of science fiction writers and futurists of past generations.

But there is an inherent tradeoff in this equation. In return for greater convenience we are increasingly losing the control over the related cyber risks.

Unlike 3G and 4G networks, which are more centralized, 5G's edge computing decentralizes processing, moving it away from the "core" of the network to the data source. This is partly what makes 5G's sub-second latency possible, but it also restricts cyber hygiene and makes the network harder to police. With thousands, or millions of devices on the "edge" of any organization's network, all making decisions at different levels of the network, all potentially serving as attack vectors for the whole organization, cybersecurity approaches of the past are becoming obsolete.

With cyber risks transcending the traditional concerns of financial and reputational impact and becoming the risks to lives, well-being or the environment, traditional cybersecurity and cyber-risk management approaches and organizational structures must be rethought.

Consumers have already proven their appetite for IoT devices. 5G will enable them to access more at lower cost. Manufacturers will continue to meet this expansive need, until we have exponential demand curves meeting exponential supply curves. Billions of devices with multiple application types – the attack vectors become limitless.

As discussed, the security of these devices is unregulated, inconsistent and unreliable. Products developed with short-term profit focus are being designed as iterative models, always released as a minimum commercially viable product. They have no defense against cyber attacks. Protection is almost impossible.

Hackers will always find a way, and with billions of entry points into the 5G network, that could spell catastrophe. We simply can't learn fast enough. As William Gibson suggests, there will be a never-ending process of adoption and adaptation as the "street finds its own uses for things."

The outcomes are frightening enough when one thinks of cyber attackers infiltrating our private networks, but what about the broader implications spelled out in Panetta's speech?

When hackers or cyber terrorists manage to compromise the systems that keep a smart city, or smart factory, or smart port, or a country functioning, the consequences are large scale and a threat to physical life. When water supply, power supply, traffic management, waste removal or connectivity are disrupted, humans suffer.

Defending ourselves against these possibilities is not a negative stance, nor is it a dampener on human progress, as some idealists would have us believe. The security of cyber-physical systems and the 5G that connects them is possibly one of the most urgent responsibilities we face in the coming decade.

A failure to enlist governments, regulators, private enterprises and consumers in a coordinated approach to the cybersecure implementation of the smart-everything world could be devastating. Not even Arthur C. Clarke could predict the results.