To: cybercommission@nist.gov

From: Sevan D. Gerard
Naval Postgraduate School
Center for Homeland Defense and Security Master's Program

Subject: RFI - Current and Future States of Cybersecurity in the Digital Economy

ROI: Research and Development

Executive Summary:

Contemporary thinking on cybersecurity issues typically involves the familiar culture of computers, of transecting wired networks of electrons organizing and transmitting the information we all create and share today and finally the privacy and economic impacts of our experience of virtual realities behind screen interfaces. We can also agree that these concerns are ubiquitous and transcend all user domains whether private, commercial, governmental or military.

There seems however to be an impending shift in the digital domain as we know it, which may prove to undermine many contemporary currents and philosophies about economics, sociology, anthropology and consequently security. Cyber technologies are being anthropomorphized and humans are being altered and augmented through the embedding of smart technologies while the buzz surrounding the growth of the Internet of Things (IoT) seldom echoes the currents of human-machine integration towards an Internet of People (IoP). These topics made good story lines for science fiction but are now merging with our reality. Technological theorists like Ray Kurzweil, Kevin Kelly or Brian Arthur have worked on defining the nature and dynamics of technology. They have speculated about the biological future of cyber technologies and on the intrinsic life within the technological ecosystem itself, which Kelly terms the Technium.[1] The future of the cyber-interface looks biologically embedded and resultantly will require an entirely new set of ideas and theories on protecting privacy, a digital economy, public safety and national security. The elephant in the room with respect to cybersecurity threats to our digital economy is the fact that cyber-technologies enable new forms of economic trade undermining what many envision as the digital economy. The normal evolution of cyber enables the development of new Shared and Knowledge Economies, which may themselves be the greatest threats to the expectations of current digital economy.

The Commission on Enhancing National Cybersecurity's interests and inquiries into future states of cybersecurity in the digital economy must consider and account for evolving usage and knowledge of digital blockchains, genetics, human-machine interfaces, technologically enhanced humans and the development of an IoP economy of distributed exchange networks and services.

The question persists and indeed grows whether the computer will make it easier or harder for human beings to know who they really are, to identify their real problems, to respond more fully to beauty, to place adequate value on life, and to make their world safer than it now is.

Norman Cousins – from The Poet and the Computer, 1966

Background

In 2013, Oxford Economics estimated the digital economy to be approximately $4.4 trillion and it has been growing at a pace of an addition $1 trillion-plus annually.[2,3] It is undeniable that as a greater segment of the world population has access to the internet, the convenience of its decentralized marketplace will attract more consumers. Obviously where there is great economic opportunity tied closely with anonymity, threats will emerge to profit or disrupt the emergent markets. The short term cybersecurity considerations for a growing digital economy must focus on traditional cyber-kill chains, network arrangements, encryption and countering social-engineering schemes. None of these schemes though appear to pose any real existential threat to the current economic paradigm, but a real threat does exist akin to an elephant in the room, which are the effects of the intended uses of cyber-technologies on market dynamics.

To better understand the potential for a categorical economic shift, two phenomenon must further discussed. The first is the merger of connected technologies, now referred to as the IoT and humans, as economic participants. The second phenomenon is the behavioral changes we are seeing on sociological scales regarding the interaction and exchanges of goods and services facilitated through cyberspace.

Science fiction seems to be catching up with reality as new internet user experiences seem to develop faster than average users can keep up with. Nonetheless the technology acceptance rate is rapidly shifting because of discoveries in medicine or experiences of augmented reality fostering a cultural shift towards embedded connected technologies with claims that the human body with be the next computer interface.[4] Progress in haptic systems, in smart materials with electromagnetic sensors, in speech recognition, eye movement and other biomechanics sensory systems are enhancing the human experience and becoming ever closer to moving into the body.[5] An explosion in neurobiology research has now opened the door to prosthetic movement through mind control. Two telling examples are the case of Nigel Ackland, who lost his arm in an industrial accident and tested out the first prosthetic arm controlled by peripheral nerves and Ian Burkhart paralyzed in a diving accident in 2010, who thanks to a computer interface linking his brain and arm became the first quadriplegic in history to regain the ability to perform complex hand and finger movements using an implanted interface.[6,7] With the seamless human-machine interface now being built, the development of implanted interfaces and nanotechnologies to allow a natural browsing experience is imminent.

Issues

When considering the cyberthreats to our digital economy, it is easy to be distracted by thoughts of some lines of code altering the normal path of High Frequency Trading (HFT), privacy and information breaches like the one conducted against the Office of Personnel Management or the overlooked siphoning of bank account decimals in the private financial sector.

The pursuit of a developing digital economy is essential because of the observable shift to online retail the world has seen over the last several years with giants like Amazon, Ebay or Alibaba. Services are seeing the same shift with Uber, AirBnB and the like. Craigslist was the first noticeable step towards a digitally facilitated P2P platform, accelerating the growth of the new shared economy. Moving to these virtual platforms for trade creates an existential threat to the standard economy as we currently know it. It also appears the the digital economy has been developing in the likes of its brick and mortar counterpart, but those dynamics are changing. Uber for example offers individuals an employment opportunity to drive customers through a new shared economy, but an interesting opportunity to many participants is that by offering to drive others, a driver in turn can get free rides. By offering this, Uber essentially is cutting out an existing slice of the transportation economy, a segment of critical infrastructure and tax revenue, by offering the same services without financial exchange. It is accomplished by shifting the economic model to a shared economy through the use of cyber technology.

The traditional economy based on the exchange of limited goods, essentially a zero-sum game, is loosing appeal with connected consumers because their economic value is improved through cyber technologies. To counter the sum-zero economic models, french philosopher Idriss Aberkane strongly supports the idea of a knowledge economy.[8] The benefits of the new economy are that unlike material goods, which are limited, material goods are infinite and their exchange multiplies the quantity rather than divide it. This is interesting because consumers' same needs are being met but through a positive-sum game. When knowledge is shared rather than a limited good, it is not split or divided but rather multiplied. This is an attractive property that is drawing more consumers to favor non-traditional digital exchanges. The price is that this undermines conventional markets, businesses and tax revenues. This shift points to a significant threat to the digital economy, not from cybersecurity attacks but the ubiquity of cyber technologies transforming the fundamental models of supply and demand. Obviously this is not a 1-2 year short term threat, but it has a significant potential to impose severe transformational pressures probably within a decade.

Having introduced the economic threats from the normal use of cyberspace we still should keep with the idea of cyberattacks as well but with a shift in mindset. As technologies become more biologically integrated, cybersecurity threats may appear to become more akin to epidemics affecting populations' health and functionality, which will require both economic and epidemiological knowledge to identify and understand. Today ransomware locks information up for financial reward, but with the progress in nanotechnology and genetic manipulation through CRISPR techniques, microbiology or genetics may become the future economic unit of exchange. If certain genes facilitate prevention or repair of conditions avoiding highly expensive and difficult healthcare, those genes may come to hold an exchange value in a knowledge economy. The biotechnology sector is already complaining that the threats to cyberspace are creating vulnerability and economic risk for those organizations providing goods and services for affected patients.[9] The sudden rise in our understanding of genetics following the success of the technologically dependent Human Genome Project, launched a healthcare revolution while

simultaneously introducing more risk into healthcare because it is completely computer dependent and therefore susceptible to cyberattack.[10]

There are numerous possibilities within the realm of cybersecurity that could lead to severe economic impacts. These revolve around the migration of technologically enhanced humans into the information cyberspace and modify behaviors of exchange.

Here is a short list summarizing a few of the concerns:

- Bioterrorism in the context of enhanced humans becomes as a cyber issue.
- Ransomware targets genetic sequestration or suspension of embedded connective technologies
- Intellectual property can be stolen through the hacking of human technological enhancements
- Increased social connectivity modifies supply and demand leading to a fundamental shift in economic models

Recommendation

Cybersecurity needs to become an independent multidisciplinary branch of science which focuses on emerging forms of the digital economy, on the future of public health, on a rapidly transforming critical infrastructure and on protecting the free exchange of and access to information.

Our inquiry into the digital economy needs to focus on its very nature. Traditional real-world economies are yielding to shared economies centered on trade, to blockchains, and to knowledge economies, none of which present synergistic profit models or dividends yet. These emerging transactional models either need to be regulated and taxed to continue funding public services, or current economic models need to be called into question and a new form of digital economy needs to be adopted.

It is also imperative to remember that as technologies evolve, they become more integrated into the human body and people may eventually navigate cyberspace natively, as an Internet of People facilitated by embedded IoT technologies. Since the IoT is hackable, people will become hackable. There are already discussions taking place about DNA forming future blockchains and with the exchange of bitcoin and counterparty blockchains online, it seems likely that a DNA blockchain with all its complexity, will also offer trading applications.[11] Another force driving the development of the human-machine interface and directly tied to the critical infrastructure sector is the harnessing of human energy to power the devices connected to cyberspace.[12] The complexity of factors pushing towards human augmentation and integrated interfaces needs special attention from cybersecurity specialists and digital economists. On a population scale, a future digital economy in a bio-integrated cyberspace where DNA forms blockchains may come to look like one where public health is a new type of currency and where cybersecurity insurance may cover healthcare problems.

The Commission on Enhancing National Cybersecurity should recommend the establishment of a grant to fund research over the next decade focusing on studying and forecasting the future of the digital economy as it transforms to adapt to a market of consumers driven by cyber exchange opportunities.

The Commission should also support a grant to fund research on the bio-integration of the IoT into an IoP, as cyberattacks on human integrated interfaces could prove dangerous to life and be highly costly.

It is recommended that the commission establish a multidisciplinary panel of experts in digital technology, systems theory, economics, genetics, biology, neurology, public health and security to forecast and conduct research on the long term effects of the normal intended use of cyberspace on a new digital economy and the cybersecurity threats created in that new paradigm.

References

[1] Kelly, Kevin. 2010. What technology wants. New York: Viking.; http://kk.org/thetechnium/

[2] https://www.ciaonet.org/attachments/18539/uploads

[3] http://www.forbes.com/sites/joemckendrick/2015/03/17/digital-technologies-will-soon-add-1-trillion-plus-to-global-economy/#731804916c6f

[4] https://www.fastcodesign.com/1671960/why-the-human-body-will-be-the-next-computer-interface

[5] http://usabilitygeek.com/what-is-the-next-frontier-for-human-computer-interaction/

[6] http://www.wired.co.uk/article/nigel-ackland-prosthetics-pioneer-wired-health-2015

[7] https://www.rt.com/usa/339501-brain-implant-man-paralyzed/

[8] http://idrissaberkane.org/index.php/en/

[9] https://www.wilsoncenter.org/sites/default/files/how_our_unhealthy_cybersecurity_infrastructure_is_hurting_biotechnology.pdf

[10] http://io9.gizmodo.com/5976845/your-biggest-genetic-secrets-can-now-be-hacked-stolen-and-used-for-target-marketing

[11] http://genecoin.me/faq.html

[12] http://www.popsci.com/environment/article/2009-01/harvesting-energy-humans