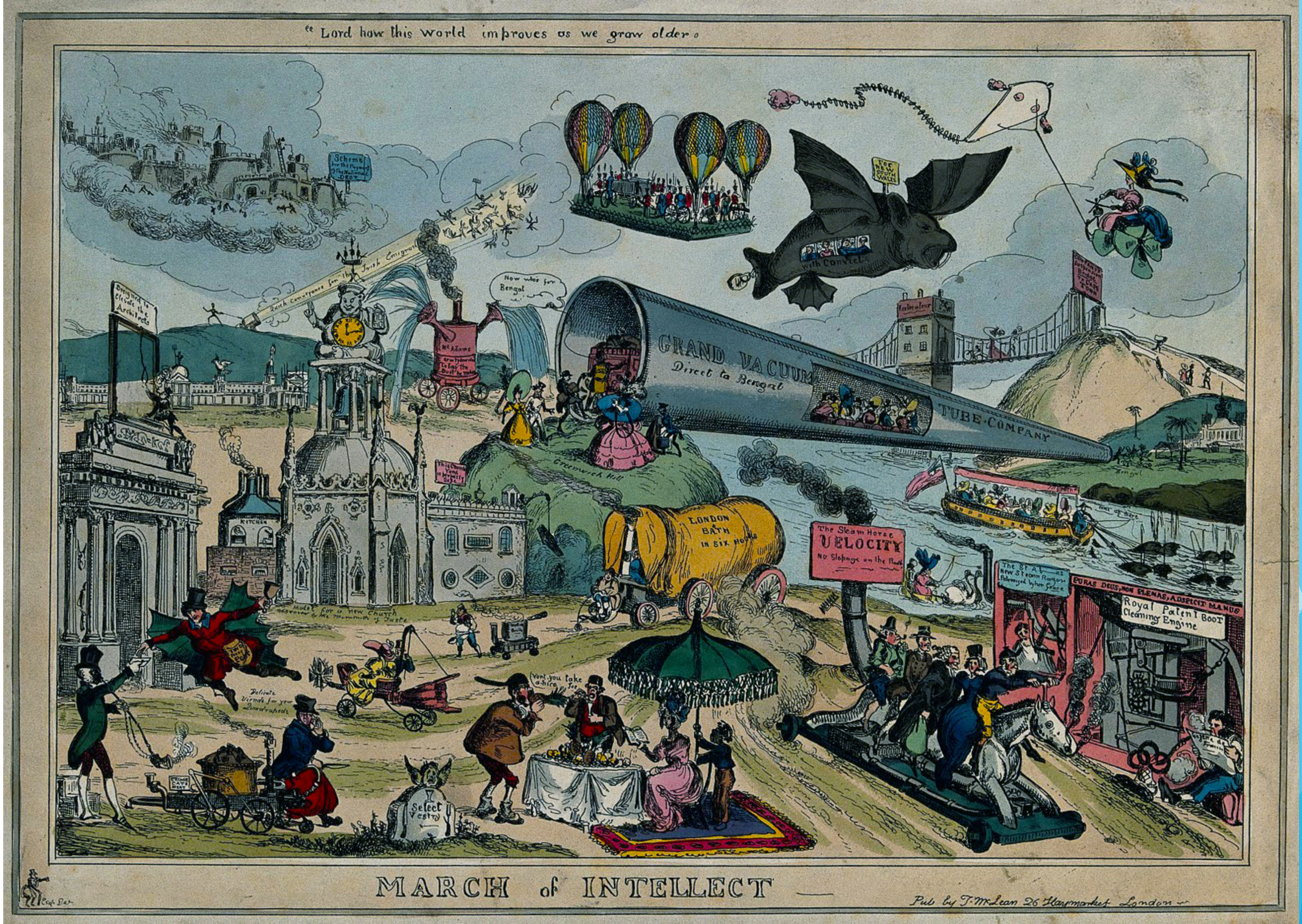
Cybersecurity: Now thru 2050

Dr. John D. Johnson

CEO/Chief Security Strategist, Aligned Security


"Lord how this world improves as we grow older."
Scheme for the Paying of The National DEBT
Quick conveyance for the Irish Emigrants
Designed to Elevate the Architects
Now who's for Bengal
McAdams
GRAND VACUUM Direct to Bengal TUBE COMPANY
FOR NEW SOUTH WALES
with Convicts
Company Suspension Bridge To CAPE TOWN
Greenwich Hill
KITCHEN
LONDON to BATH IN SIX HOURS
The Steam Horse VELOCITY No Stopage on the Road
New Steam Rangers Patronised by her Grace
PURAS DEUS, NON PLENAS, ADSPICIT MANUS
Royal Patent Boot Cleaning Engine
Bengal
Model for a new Church
Delicate Viands for your Quadrupeds
Vont you take a hire
Select Vestry
MARCH of INTELLECT
Pub by T. McLean 26 Haymarket London

Today’s Trends and Attacks: *Fast & Furious*

- State sponsored events increasing; Cyber attacks mean big bucks for criminals
- Ransomware/Cryptocurrency mining on IoT
- DDoS attacks > 1Tb; leveraging botnets of traditional computers and IoT
- Rise in regulatory risk
- Human-Automation attacks (e.g. MS Help Desk)
- Moving data to the cloud can lead to exposure (new environment, new tools, misconfigurations, lack of controls)
- It still takes 191 days to detect a breach
- Blockchain/Cryptocurrencies still have weaknesses in their models
- We are still bad at situational awareness
- CISOs still need to do a better job to explain and report risk to the BoD
- Program maturity is not sufficient; need to focus on cyber resiliency
- IT staff doesn’t understand OT problems/protocols
- Lenient BYOD policies
- Need to identify and locate and classify our data; achieve compliance; manage ethically as data steward throughout data lifecycle
- THREATS OUTPACE CAPABILITIES!!!
- INTERCONNECTION AND COMPUTING CAPABILITIES ARE FORCE MULTIPLIERS FOR ADVERSARIES!!!

In the future… everything is connected…

Everything is at risk.

- me

What do Futurists think 2050 will look like

- Climate: Hotter, Possible Coastal Flooding, More Extreme Weather, Loss of Glaciers, Transportation Across Poles, Water Shortages
- Population: 9.5 Billion people, more urban crowding (70% urban)
- Food: More people means more food required; more protein; (70%)more food with no more (or fewer) farmable acres
- Species: More extinct species, acidation in ocean may reduce commercial fish supplies
- Politics: A big question!!! Small wars? Big wars? More trade? Definitely not a US-Centric world from a trade perspective. Will the US still take a leadership role from a military standpoint?
- Longer lives mean MANY more older people
- Diversity in culture, language

The slippery slope of technology…

- It is said that one human year is equivalent to 7 ‘cyber’ years, or technology years. So, technology is advancing faster and faster.
- More data was created in 2017 than in the past 5,000 years.
- The technology that will shape the future, includes the technology we know and have built upon in the past 50 years, but also many emerging technologies which we know about and which we don’t yet realize is on the horizon. These technologies will be revolutionary, in the way that the microchip was revolutionary.
- When we hit a limit with making chips smaller because of quantum effects, scientists developed new methods to drive the computer chip smaller.
- Storage is getting much smaller. A team of physicists in the Netherlands have developed a storage device composed of chlorine atoms on a tiny metal surface that could in perhaps 10-20 years be scaled up to hold about 10 terabytes of data on a 1cm square space. By 2030, electron spin may replace magnetic storage.
- We know that in our genes, DNA is used to store data. In 10-20 years, the letters A, C, T & G may be used to encode data commercially for long term storage, and by 2050 we may be adding information to our own genes as. Imaging using your own DNA to store all of your PHI.

Future and why we need AI to work…

- AI is a buzzword, and we all have a slightly different interpretation of what AI and ML mean, but there is know doubt that AI is something that will revolutionize our world and how we perform our cybersecurity duties.
- In the next few years, we will find more mature AI solutions to help us address the flood of events as our sensors collect more data. Threats will increase exponentially. It was mentioned we cannot understand exponential growth well. This means if we need 1.3 million new cybersecurity professionals in 2019, that there is no way we an keep throwing human beings at the problem. The problem will only get worse, as the volume of attacks, the velocity and voracity and sophistication increases year after year. I claim that we need AI to detect and aggregate and pass along actionable information to humans.
- When we look at the ICS-SCADA and operational technology; We have well-trained IT professionals who have no idea what OT is. It is said there are only 1000 OT experts in the country.
- As we look out a decade, perhaps we will start to see a real hybrid with AI and humans interfaced, because the human mind is still really really good at identifying patterns and making connections. Think how much better our SOC analysts can be with AI to help filter data and provide immediate details, and then automation and orchestration to quickly and effectively respond.
- Today, adversaries are leveraging automation and AI to attack us.
- In 10 years, the adversary and the defender will be be battling their bots. My AI vs your AI.
- By 2050, humans will only be involved in training the AI, and at the high level setting policies on how to respond.

What other advances will change our lives?

- Big Data will get bigger: this will lead to targeted marketing that will annoy you, but it will also help you maintain your health and live longer
- Relevant to cybersecurity, these diverse data sets will need to be understood and managed, and the aggregation of these datasets are already impacting our privacy and in the next few years we will see how important data management is, in relation to privacy regulations such as GDPR.
- Globally, we treat privacy and intellectual property differently in different regions and with different cultures.
- We tend to focus on the technology but we need to remember it's about people too.
- I see the perimeter evolving from the enterprise to endpoints, and eventually to the data itself. I don't know how that will be done.
- I see all the network data from all the billions of devices communicating being huge. There will be a glut of devices. Establishing authenticity will be vital. In 10 years we may have global connectivity with high data rates by satellite. This will impact politics and cross borders.
- 3D Printing: From the atomic scale to building houses and Moon bases.

More thoughts on technology…

- Blockchain will grow up in the next decade and be used to maintain integrity in everything from server logs, to elections, to preventing prescription fraud. By 2050, cryptocurrency will be the default method of payment.
- IoT will keep growing, and continue to be difficult to defend in the next decade. While we have grand ideas for how to protect legacy IoT systems, in 10 years we may be looking at protection being an abstraction layer.
- Our networks will change. In 10-20 years, everything will move to the cloud. We will start with diverse controls and SecOps. In 10 years we will move our controls to mature cloud security solutions.
- Quantum Computing is already commercially available and will be common in just a few years. In 20-30 years, it may be used for unanticipated purposes, good and bad. It puts all of our past and future encrypted secrets at risk of being exposed.

Let’s start with transportation as an example

- Transportation: Autonomous Vehicles (AV) (air/land); with wireless communications, advanced sensors, AI… we will see trucking and shipping and farming become automated. Great benefits/efficiencies; Risk of high impact attacks.

  Flying Uber will be safer than AV on legacy roads and highways. In the short term, AV will be relegated to designated lanes. In 20 years, I expect to see fully AV and assisted AV in many urban and well managed locations.

  It is possible that even before 2050, the “flying Uber” may prove safer and more reliable than “legacy Uber”.

- We still have many environmental and external threats that will always exist, and many which may be eventually mitigated: Weather, turbulence, old infrastructure. As well as cybersecurity threats. We have seen some of the cybersecurity attacks that might exist, but no doubt there will be many more advanced threats in the future.

My AI Buddy…

- I predicted this in 2000 and feel we are very close to the first ML buddy for little children.
- Initially, it will be responsive, in 20 years it will be predictive.
- This is an Internet connected device with a furry, friendly skin. Your children start off with it monitoring them in their cribs. Eventually, it help teach them to talk. It answers their questions. No need to remember anything, my Furby will fill in the blanks.
- As the child grows up, the AI becomes more sophisticated. Keeping them safe, helping them learn.
- Eventually, the teddy bear is gone, and the AI buddy is in their ear, always on their shoulder helping answer their questions and helping them make decisions.
- From cradle to grave, we will imprint with our own AI. We don't need it to pass the Turing test, we just need it to be smarter and smarter AI/ML.
- The unanticipated technology that will be an everyday part of our lives, will offer great benefits, but can also expose or harm us in much more severe ways.
- The use of technology involves trade-offs. The better the security and privacy controls are baked in and the better options adults have to manage their privacy and safety, the better the outcomes.

Future Human Technologies…

- Personal Health: More sensors means better management of your health. Also, means your doctor will tell you what to do and if you don't your insurance rates will jump up. Hacking of your devices can affect your insurance and your life. Hospitals will have IoT and devices to monitor and regulate your health. This puts life and privacy at risk from attacks.
- By 2050, human cybernetic augmentation will be common. This may lead to better health, cognitive augmentation, as well as cosmetic surgery. This might be as common as tattoos in 2050. What you can't electively do in the US, you can get done in a back alley in a country with fewer regulations.
- Human implants and augmented eyes/contact lenses will allow you by 2050 to view the world the way you want. A skin, akin to rose colored glasses. This takes augmented reality to a new level. You will choose how you want others to see you, in the real world.
- Biometrics will probably replace passwords in the next decade. Multiple factors will be used to evaluate your risk score when you connect to a device or initiate a transaction. It will be invisible to the end user.
- In 20-30 years, very realistic, humanoid robots will be common. The AI will be fairly advanced by 2050.

Developing Nations

- In the immediate future, technology will benefit developing nations, with no real infrastructure and capabilities.
- m-Services have been helping people in these countries for years. Older devices. Messaging and services for voting, banking, sending funds, getting information and maintaining their health.
- Villages with no wired infrastructure can leverage cellular and bypass the need to build out a telecom network like we did.
- Technology is bringing electricity and clean water to remote sites.
- Flying vehicles (autonomous “drones”) may be safer and bypass the need to build out and maintain physical road infrastructure.
- As we know, these all have environmental concerns and because they are networked, they are at risk of attack.

Implications of Automation

- In the next decade, we will see hourly wage earners displaced by automation. We saw this as factory workers were laid off in the 1980s, due to factory automation. In 10-20 years, we may see automation displace factory workers, farm workers, retail/food/hospitality workers displaced.
- In 10-30 years, many blue and white collar workers will be displaced and need to be retrained.
- Our ability to retrain and educate our workforce will be critical, in order to transition people from all the common jobs that won't exist in the future, to jobs that don't yet exist.
- This leads to a new technical caste system. Those who understand technology, and those who don't. Technology will increase the digital divide, and may lead to a shorter work week, or a dystopian future with high levels of unemployment.

Human Behavior, Values, Privacy, Policy

- Humans still behave like humans in the future.
- Today we see technology to make videos which are indistinguishable from reality. This trend will increase and the Nigerian Scam will be replaced by phishing and social engineering which is much more sophisticated and harder to detect. This is the #FAKENEWS problem.
- Commercializing technology is one hurdle. It takes time for mass production and prices to drop.
- We may find resistance due to safety perceptions. After all, we operate with human biases and we tend to trust ourselves more than machines, regardless of the statistics and scientific facts.
- Overcoming our human resistance is a cultural issue. With time we grow to accept new ideas and new technology. The way we think about technology doesn’t change in a linear fashion, it advances generationally.
- Government agencies will put a damper on the rapid adoption of new technology. Think of drug testing. But, on the other hand, look at the effect Elon Musk and others have had at advancing wild ideas like, self-driving cars, electric vehicles, rapid transportation (hyperloop), and sending humans to Mars.
- God Bless eccentric billionaires. At this rate, I have no doubt that by 2050 we will be actively mining asteroids.

Ethics

- **Technology advances much faster than our ability to ethically use it and appropriately regulate it.**
- Privacy was really only codified in the past century.
- We need to ask if we have lived through the "golden age of privacy" and if in the future privacy will be a thing of the past.
- Privacy controls may need to be baked in, opt-out not opt-in. But that can lead to overhead and inconveniences to consumers. If we don't force users to operate with significant privacy controls, do we then try to overregulate to "get privacy back"? Can privacy be gotten back? I think with certain information, when the cow's left the barn, you aren't getting it back.
- Maybe the future generations will accept functionality and "free", and allow marketing and we will move to a much more transparent society.
- That can be great, but in reality with 9 billion people by 2050, it sounds like a hard journey to maintain privacy and avoid a Big Brother state.

Fundamental Changes?

- **Do our existing protocols and methods serve us in the world of 2050?**
- **Does CIA still hold?** I think it will need to be redefined.
- **Our networks will evolve**: ad hoc, mesh, edge, and, as our devices get smaller: mobile, grain sized computers in the next 10-20 years, and eventually by 2050 a fully ubiquitous computing environment where computing is a utility.
- **Technology will be pervasive by 2050**. It will be woven into the fabric of our society. It will become invisible. Our grandchildren and their grandchildren will come to see technology as so small and complicated that it is indistinguishable from magic. It will be black boxes, like a car engine is a black box. This is a generations separation from knowing how the world around us works. It is black boxes all the way down.
- Ultimately, we are thinking today about protecting tomorrow, based on what we did yesterday. Will we be able to adapt our thinking fast enough, if technology and threats really accelerate along a hockey-stick model??

Implications

- Computer-Human interfaces will melt away by 2050. Technology will not just be a part of our lives, it will be a part of our bodies.
- The implications are that we will be so dependent on technology that if it were ever to be shut off, our society would shut down, and so might our 3D printed, cybernetic body parts.
- By 2050, barring society taking a radically different direction due to war, famine, biological, natural disasters, solar flares and asteroid hits, our dependence on technology along with the importance to our economy and lives, the impact of a successful cyberattack can be much more dire than an attack on critical infrastructure today, which itself can be severe. Computing and networking and technology can give a nation state the ability to attack and cause havoc, from around the world. This risk will only grow.
- The threat of INFOWAR is very possible now, and it dramatically increases as we approach 2050.
- Thus, our jobs will be harder, and we must rely on technology to safeguard technology.
- Computing and technology will be invisible, cybersecurity needs to be invisible and at a low level and work reliably. This really motivates me to think about making dramatic, fundamental changes to how we network devices using protocols that were not designed to be secure.
- The alternative is to use legacy protocols and continue to chase down the bad guys. The challenge of attribution and legal or military action.

“We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction.”

– Bill Gates

Links

- https://youtu.be/HipTO_7mUOw Future of Autonomous Weapons
- https://www.youtube.com/watch?v=ozLaklIFWUI Microsoft Future Vision
- https://www.youtube.com/watch?v=OptqxagZDfM A Day in 2020
- https://www.youtube.com/watch?v=d36M4CCCXRw Tomorrow’s Connected Home (Beko)
- https://www.youtube.com/watch?v=g_1oiJqE3OI The World 2050 (BBC)
- https://www.fox.com/watch/39b3ae45d91f1e826f679ad8555a5a33/ X-Files (Season 11 Ep.7) “Rm9sbG93ZXJz”