BRIEFING NOTES

#BN-36-Space and Cyberspace-Feb2021

TOP 10 CYBER DEFENCE PREDICTIONS BY CLAIRVOYANCE CYBER CORP OF 2021

Author: Dave McMahon
Clairvoyance Cyber Corp
www.clairvoyance.network
info@clairvoyance.network
819.664.2708

"The next natural disaster or pandemic will trigger violent digital transformation, the result of which is that everything will be mediated by cyber technology. Meanwhile, our adversaries will choose this time to strike western democracies with cyber exploitation, misinformation campaigns of chaos while criminally capitalizing on the events and purposefully interfering within critical infrastructure sectors including: healthcare, emergency services, industry and defence. The capability of organizations to operate securely outside of the conventional office, adapt business processes to the cloud, adopt next generation secure cyber technology and recalibrate to the new reality, will be put to the test." – January 2020 Cyber Defence Prediction by Clairvoyance Cyber Corp

Dramatic digital and social transformation will continue as governments oscillate between re-opening and lockdown owing to the pandemic. Adversaries will take advantage of this ambiguity and instability by propagating misinformation, mounting destabilization campaigns, interference in critical infrastructures, defence supply chains, with disruptive cyber attacks and conducting systematic espionage while institutions are in flux.

Remote work solutions will be rolled out by central government but may not full satisfy the operational requirements of the military and may be vulnerable to exploitation. The lack of routing integrity and infrastructure governance will become the primary attack vector particularly in forward deployed operations. A shadow network of personal devices and apps will emerge as an alternative means to communication and collaboration. The line between professional and personal lives will blur.

Secure cloud computing will rocket in importance and uptake by the armed services and members of the military. This will provide much improved capability, resiliency and security at the fraction of cost of traditional architectures, but will challenge conventional doctrine.

5G will be completely deployment across Canada this year and will pave the way for the Internet-of-Things. The impact to individual member's behaviour and the military enterprise will be significant. The convergence of multiple industrial sectors and regulatory environments accelerate.

Industrial cyber power will continue to grow and will challenge traditional Westphalia models of governance and sovereignty, thus necessitating a new social contract and renegotiate equities for public private partnerships and Civil-Military Co-operation (CIMIC). The private sector will conduct more military-like active cyber defence and persistent engagement operations independently and in cooperation with the state, in order to defend the country.

The war on information and truth systems, science and reason will emerge as one of the most significant challenges of our lifetime. The leadership vacuum in this space will become increasingly problematic in dealing with misinformation as a domestically and conducting information peace-keeping (IPK) operations abroad.

Artificial Intelligence particularly as required to moderate Internet content, will drive social scientists, philosophers, civil society, privacy authorities and legislators to better define a set of universal values, ethics and norms so they engineers can code the machinery of cyberspace. Engineering necessity will thus drive social science.

Attacks such as Solar Winds (and ASN.1 previously) will highlight supply chain defence, mission assurance, the importance the critical information infrastructure interdependency and understanding complex systems. There will be increased pressure for defence industry verticals and the military to collaborate on sovereign solutions.

The contest to control and influence the fabric of cyberspace will be as significant as the Manhattan project. China will seize vital high ground in cyberspace globally; seek control of big data, core internet infrastructure, Artificial Intelligence, Quantum Computing, and fifth generation mobile communications initiatives including launching low orbit 5G satellites over Canada. China's Road and Belt Initiative will shift the balance of economic technological and military global power. A China and Russian alliance in cyberspace will see Russian Gerasimov doctrine for hybrid warfare leverage China's Three Warfares Strategy, Hundreds Talents Plan, United Front, and Road And Belt Initiatives. A digital iron curtain will balkanize cyberspace into East and West.

China and Russia will leverage industry, government, military, intelligence services and organized crime to expand state power and influence cyberspace. The Kremlin's reliance on proxies, weaponized disinformation, cyber disruption and deception measures will operate just below a level-of-armed-conflict. Meanwhile China will continue to conduct aggressive cyber espionage against Canadian businesses steal intellectual property as part of efforts to re-innovate critical technologies.

ACTIVE CYBER DEFENCE PREDICTIONS

- The gap between offensive capabilities and a traditional cyber security response will continue to widen.
- Industry will be a proxy target of Hostile Intelligence Services and Militaries who will continue to exploit, interfere and influence Canadian interests.
- Organization will require sophisticated hunt capabilities to interdict Advanced Persistent Threats that are undetectable by traditional cyber security.
- Disinformation campaigns in social media using semantic botnets will continue to rise in strategic utility of threat actors.
- The Internet will continue to enable the ability to malicious actors to influence populations at scale.
- Industry will be compelled to take a more foreword-leading stance in active cyber defence

2020 PREDICTIONS

2020 will continue to see changing demographics, resource competition, environmental stresses, globalization, economics, and increased urbanization. Meanwhile, unprecedented advancements in science and technology, will shape the future cyber security environment.

A rapidly globalizing world will pose significant challenges to Governance. Power will continue to diffuse amongst corporations, empowered individuals, civil society, criminal organizations, and peer and near-peer nation-states. The power-shift will be particularly acute in the cyber domain and will precipitate a re-adjustment of Westphalian models towards a new construct.

Traditional forms of hard and soft power wielded by governments will prove less influential. National governments, if they are unable to adapt and respond to power-shifts accelerated by digital empowerment, will find themselves overcome by non-state actors usurping national control. Attempts to regulate Cyberspace or establish norms will not be realized.

Open media, big-data, ubiquitous mobile communications and the IoT will be central to security and privacy issues. Contrarily, open access to the Internet will continue to be challenges by nation states seeking to regulate, balkanize, block, censored, shape, controlled and deny environments. The interests, values, norms and strategy of the Western liberal democratic vision of open networks and Internet freedom, will be countered by alternative models posed by states seeking to restrict and control the Internet along nationalistic boundaries. Norms and legal framework will struggle to keep pace with rate of change, or will fail completely in some environments.

Post Snowden distrust of Western technology will continue to contribute to the colonization of developing-nation's information infrastructure by Eastern suppliers. There will be a corresponding negative impact on human rights in those regimes.

China will continue to 'legitimately' expand its state surveillance footprint into the West through the sales of mobile devices, 5G infrastructure, forward routing points-of-presence and mobile apps. whilst covertly engaging in DNS poisoning/rerouting and targeted attacks against strategic targets using persistent malware, supported by traditional espionage.

We will continue to experience rapid convergence across multiple domains were social media will provide a frictionless state between the Human terrain, the Network and Internet-of-Things. Cyber will become an Internet-of-Everything.

Cross-domain risk will contribute the greatest impact on governments, businesses and citizens. Nearly all cyber compromises will be socially engineered. The largest magnitude denial of service attacks will come from the Internet-of-Things. Cyber weapons will increasing generate kinetic and semantic effects.

There will be a tighter connection between influence activities, network attacks and physical effects. The complexity of cyber defence will become out-of-reach of all by the most sophisticated organizations and talent. Meanwhile specialization will not solve the cross-domain challenges or build the systems-of-systems required for remediation. There will be an increased requirement for deep generalists and poly-disciplined teams.

The breathtaking fusion of the cloud, big data, genomics, 5G, artificial intelligence and wearables will be game changing. Mobile computing, social networks and the Internet-of-Things (IoT) will have triggered the rapid inflation of the digital universe.

The wrist-watch will lead wearable computing trend and become a vector for attacks.

The immediate future in cyber security will be influenced by: big data science, artificial intelligence, internet-of-things, cybernetics, social networks, 5G, quantum, and cloud. More significantly will be an understanding the emergent effects of these technologies within complex systems such as critical infrastructures and socio-technological networks.

Innovations of virtualisation and software-defined networks, had driven the data to central computing fabric. The next oscillation will be with 5G, IoT and IPv6 precipitating an accelerated growth of the Internet. Computing will be pushed back to the edge where the data will then reside in the sensor fabric. We can expect to see increased important on the security of decentralized AI, fog computing, mesh, and agile networking.

Machine telemetry will rival human communications just as metadata may prevail of over data in quantity. The Internet-of-Things (IoT) will expand a domain previously inhabited by humans to one that is shared with machines. The legal definition of communications will be tested in the courts.
The largest mobile device will be your car. Cyber security for the automobile industry will lag vulnerabilities and threats in this space.

The war on truth will continue but the investment by commercial providers to curate content will begin to take hold. Meanwhile, this pressure for upstream security monitoring will upset net-neutrality.
The integrity of algorithms, AI/ML and autonomous processes will come under increased scrutiny by security and privacy communities.

Mass ransomware extortion e-mails will continue unabated.

Russia and China will continue to launch increasing sophisticated and aggressive attacks against Western interests, despite agreements to the contrary.

Six-generation malware will stress traditional IT infrastructures to the brink; precipitating a complete rethink of cyber security and bolstering the business case for active cyber defence.

China will invest heavily into quantum computing, artificial intelligence, big data and 5G technologies whilst clandestinely targeting those technologies and markets.

Russia will continue to tune hybrid/informationalized warfare, based upon the Gerasimov Doctrine. Influence operations will be empowered by covert cyber and human operations in response to geo-political or military objectives.

China will seek to gain competitive advantage in global IT market by legitimate and prohibited means. We can expect asymmetric escalation in response to Canada taking measures to protect our supply chain, including an uptick in cyber attacks and harassment of Canadian citizens.

The concept of hack-back will be revisited in the context of gathering evidence for effective prosecution by the private sector. Commercial entities will continue to lead attribution efforts in this regard.
Cyber intelligence will have a shorter shelf-life. There will be increased pressure to act on intelligence in a timely manner with demonstrable effect. Cyber security and defence programs will be obligated to calculate economic efficacy.

Smart cars, homes and medical devices will be harvested as part of a botnet of significance.
We will see the emergence of mega smart cites and other hyper-sensored environments.
Artificial Intelligence for cyber defence will lead the offensive use of AI.
Networks of importance to the country will emerge.

Hunt and adversary pursuit capabilities will become marketable by many but delivered by few.
Mandatory breach notification will have mixed consequences. Organizations may turn off sensors or choose not to pursue leads for fear of discovering a breach. The requirement to disclose a breach may interfere in major investigations and the sharing of threat intelligence.

There will be a renewed impetus for cyber security programs, in both public and private sectors, to table tangible economic industrial benefits and return-on-investment.

Crypto currency will remain important to cyber crime.

The private sector will lead in counter-influence and radicalizing programs in domestic and global arenas.

Foreign and domestic actors will attempt to interfere in the next Canadian election using an online influence and deception campaign facilitated by network exploitation.

Staging malware will likely be discovered within the CI supply chain, signalling purposeful interference.