Photo courtesy of Shutterstock

A cyber resilient world

Cybersecurity is old hat; we all understand why it's important to protect our data from those with malicious intent, and most people are aware of the large-scale attacks on commercial corporations, governments and defence, and the need for these groups to protect themselves too. Cyber resiliency, namely built-in resistance to cyber-attacks, is becoming increasingly prevalent throughout the commercial and government worlds, responding to the ever-growing threat we face today. Jill Durfee, Technology Correspondent explains.

The level of connectivity available today has completely revolutionised the way the world works. From how we manage our banking, utilities and shopping through to socialising, entertainment and travel etc., the world is a very different place to the one we lived in just ten years ago. Being able to manage so many different aspects of our lives online comes with its own risks though; instead of violent crimes such as theft, consumers are increasingly at risk from cyber criminals, who hack bank accounts and send out phishing emails; likewise, identity thieves no longer have to go dumpster diving for discarded bank statements, since they can now find all this information online, with only a small amount of knowledge and skill.

For the average consumer, it can be a living nightmare for years to recover from identity theft or hacked banking details. However, the implications for government and defence are much more severe. Should one piece of data be misplaced or stolen, the ramifications can be extremely wide-reaching, and in some of the more extreme examples, life-threatening for hundreds or thousands of personnel. Never before in history has data security been such a vital aspect of day-to-day operations within government and military spheres. Everything from troop movements, voting systems and the location of top-secret materials is at stake.

Of course, one of the biggest challenges in cybersecurity is the rapidly evolving nature of security risks. Simply speaking, threats are advancing faster than we can keep up with, and there is no one-size-fits-all cybersecurity solution. Indeed, effective cybersecurity includes a collection of technologies and processes to protect networks, programmes, computers and data from attack or unauthorised access. Both physical and cyber threats must be guarded against to ensure the essential delivery of services. Accordingly, governments must focus on all aspects of cybersecurity, and retain advice and technologies from a variety of vendors. This can lead to complicated systems with a very large number of players working to different levels, leading to confusion and ineffective coverage.

GaN BUCs

for your mission-critical applications

The last word in GaN BUCs from the first name in HPAs.

- 80 W to 100 W in C-band
- 25 W to 80 W in Ku-band
- 10 W to 200 W in X-band
- 160 W in Ka-band

10 W X-band Transceiver

160 W Ka-band GaN BUC

Download our app! Search: CPI

Download on the App Store

GET IT ON Google Play

CPI
Communications & Power Industries

CPI Satcom Products | www.cpii.com | satcommarketing@cpii.com. | 1 (669) 275-2744

Cyber-attacks in 2019

According to the Centre for Strategic & International Studies (CSIS), 2019 was a big year for digital breaches, with the following highlights reported:

- **January:** US prosecutors unsealed indictments against Huawei and its CFO Meng Wanzhou alleging crimes ranging from wire and bank fraud to obstruction of justice and conspiracy to steal trade secrets.
- **February:** Prior to the Vietnam summit of Kim Jong Un and Donald Trump, North Korean hackers targeted South Korean institutions in a phishing campaign using documents related to the diplomatic event as bait; state-sponsored hackers were caught in the early stages of gaining access to computer systems of several political parties as well as the Australian Federal Parliament.
- **March:** North Korean hackers targeted an Israeli security firm as part of an industrial espionage campaign; Russian hackers targeted several European government agencies ahead of EU elections; the UN Security Council reported that North Korea had used state-sponsored hacking to evade international sanctions, stealing US$670 million in foreign currency and cryptocurrency in 2015-2018; following an attack on Indian military forces in Kashmir, Pakistani hackers targeted almost 100 Indian government websites and critical systems - Indian officials reported that they engaged in offensive cyber measures to counter the attacks.
- **April:** Ukrainian military and government organizations were targeted as part of a campaign by hackers from the Luhansk People's Republic, a Russia-backed group that declared independence from Ukraine in 2014; hackers used spoofed email addresses to conduct a disinformation campaign in Lithuania to discredit the Defense Minister by spreading rumours of corruption; the Finnish police probed a denial of service attack against the web service used to publish the vote tallies from Finland's elections; Iranian hackers reportedly undertook a hacking campaign against banks, local government networks, and other public agencies in the UK.
- **May:** The Israeli Defense Forces launched an airstrike on the Hamas after a failed attempt to hack Israeli targets.
- **June:** The US launched offensive cyber operations against Iranian computer systems used to control missile and rocket launches; Iran announced that it had exposed and helped dismantle an alleged CIA-backed cyber espionage network across multiple countries; government organizations in two Middle Eastern countries were targeted by Chinese state-sponsored hackers.
- **July:** Capital One revealed that a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers; encrypted email service provider ProtonMail was hacked by a state-sponsored group looking to gain access to accounts held by reporters and former intelligence officials conducting investigations of Russian intelligence activities; a Chinese hacking group targeted government agencies across East Asia involved in information technology, foreign affairs, and economic development; Libya arrested two men who were accused of working with a Russian troll farm to influence the elections in several African countries; Croatian government agencies were targeted in a series of attacks by unidentified state-sponsored hackers.
- **August:** China distributed malware to Uyghur populations using previously undisclosed exploits for Smartphones; Chinese state-sponsored hackers targeted multiple US cancer institutes to take information relating to cutting edge cancer research; North Korean hackers conducted a phishing campaign against foreign affairs officials in at least three countries, with a focus on those studying North Korean nuclear efforts and related international sanctions; Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications; the Czech Republic announced that the country's Foreign Ministry had been the victim of a cyberattack by an unspecified foreign state; networks at several Bahraini government agencies and critical infrastructure providers were infiltrated by hackers linked to Iran; Russian hackers used vulnerable IoT devices like a printer, VOIP phone, and video decoder to break into high-value corporate networks; a seven-year campaign by an unidentified Spanish-language espionage group resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army.
- **September:** Huawei accused the US government of hacking into its intranet and internal information systems to disrupt its business operations.
- **October:** An Israeli cybersecurity firm sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp; a state-sponsored hacking campaign knocked more than 2,000 websites offline across Georgia, including government and court websites containing case materials and personal data; the NSA and GCHQ found that a Russian cyberespionage campaign had used an Iranian hacking group's tools and infrastructure to spy on Middle Eastern targets; Chinese hackers targeted entities in Germany, Mongolia, Myanmar, Pakistan, and Vietnam, individuals involved in UN Security Council resolutions regarding ISIS, and members of religious groups and cultural exchange non-profits in Asia; Iranian hackers conducted a series of attacks against the Trump campaign, as well as current and former US Government officials, journalists, and Iranians living abroad.

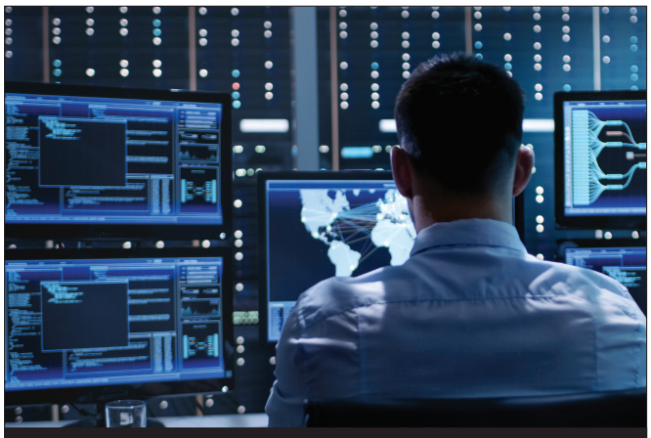

Photo courtesy of Shutterstock

WHY COMPROMISE WHEN YOU CAN HAVE IT *ALL*?

Multiprotocol
Management & Diagnostics

Complete Feature Set

Superior RF Performance

Ultimate Reliability

SATELLITE 2020
BUILD . CONNECT . UNITE .
BOOTH 425

TERRASAT Communications, Inc.
Engineered to Endure

Explore all **IBUC** models at
TerrasatInc.com

- **November:** Iranian hackers targeted the accounts of employees at major manufacturers and operators of industrial control systems.

The common thread amongst the above highlighted stories is one of Chinese and Russian, often state-sponsored, hackers attempting to gain extremely secure information vital to national security and intellectual property. Of course, many more countries have also been named as taking part in cyber-attacks last year, and the conflict with Huawei is still yet to be resolved satisfactorily. The nature of the threats – election rigging, theft of sensitive IP, the dissemination of false news, and out-and-out government and individual espionage – is a particular concern to us all.

Assessing cyber resiliency

Cyber resiliency is becoming an increasingly important topic when it comes to the cybersecurity environment, particularly within the government and defence sectors. With resiliency built-in, more attention can be focused on the more skilled and high-threat attacks, while less serious or well-planned attacks are naturally rebuffed.

Photo courtesy of Shutterstock/Titima Ongkantong

Indeed, the US Government in particular is renewing its focus on cyber resiliency, particularly on the weapons front, with the 2016 National Defense Authorization Act requiring all weapons to start to be assessed for cyber vulnerabilities. While thousands of companies across the world hold competency and even excellency in protecting computers and networks from cyber-attacks, there are in fact very few equipped with the expertise to perform the same task in complex weapons systems. In line with this act, Raytheon has won contracts to find and fix cyber vulnerabilities in the US Air Force's F-15 fighter and C-130 transport fleets, although much about the deal remains confidential.

Another entity working with the US Government on cyber resiliency is Lockheed Martin, which in August 2019 piloted a first-of-its-kind model that standardizes how to measure the cyber resiliency maturity of a weapon, mission, and/or training system anywhere in its lifecycle – the Cyber Resiliency Level model (CRL). Cyber resiliency, the ability to anticipate, withstand, recover from and adapt to changing conditions in order to maintain the functions necessary for mission effective capability, has until now lacked a common method for its discussion and assessment.

To apply the model, engineers work with US and allied military program stakeholders on a series of risk and engineering assessments. The CRL provides increased visibility into the current state of risk and produces a customized, risk-mitigation roadmap that shows how to increase a system's CRL to a more desirable level.

"Today's software-based military systems and a global supply chain make securing military systems a complex problem to solve," said Jim Keffer, Director of Cyber, Lockheed Martin Government Affairs. "With the CRL, we can now leverage existing risk management frameworks to effectively measure and communicate resiliency across six categories we know are important to our customers. The release of this model builds on Lockheed Martin's enduring commitment to mission assurance and will ultimately help the warfighter operate in cyber-contested environments."

A secure future

Cybersecurity has never been as important as it is today. With attacks becoming increasingly sophisticated, and the number of hackers, particularly state-sponsored, growing at an alarming rate, the threat level is on the rise. The physical battlefield is now just one aspect of the warfighting arena, with digital playing an increasingly significant role in a nation's domain.

Malicious attacks on government and defence sectors, as well as on commercially sensitive private entities, are growing into a larger challenge than any time before in history. While training and new cybersecurity tools are on the up in almost very sector, intruders too are getting to grips with new tools and techniques for causing havoc.

Increasingly, networks, systems and software are being designed with cyber resiliency built in, while older hardware, such as vessels, tanks and aircraft, are having assessments and fixes being built in ad hoc. Accordingly, prices are on the rise and demand is booming; great news for commercial entities operating in the cybersecurity sphere, but not so good for those governments who have to find increasingly large amounts of funds.

www.gazprom-spacesystems.ru

GAZPROM
SPACE SYSTEMS