Photo courtesy wutzkohphoto/Shutterstock

Homeland security - protecting against cyber threats

In today's world, we are more connected than ever before in history. We can do so many things online; keep in touch with loved ones, consume the latest film and music media, essential banking, pay bills, shopping, and even work. As such, cybersecurity has become a major part of our lives. Every individual must remain vigilant to protect their identity and financials from those who would use them for themselves. On a national level, cybersecurity is even more important. Governmental organisations depend on a safe and stable cyberspace to keep our countries safe from a whole host of groups who would wish us harm.

Cybersecurity has become a key part in all our lives today. It's vital that we keep personal information secure that others could use against us; this extends to both the individual and the state.

For governments, the era of connectivity has created massive new security challenges. While we've progressed incredibly in terms of the amount of information that can be collected and communicated over the Internet and other wireless feeds, giving us greater capabilities than ever before, it's imperative that this information remain in the intended hands. If information on troop movements or plans are acquired by the enemy, the battlefield becomes all the deadlier. Meanwhile, if malicious groups gain access to governmental voting systems, democratic process is in great trouble.

One of the biggest challenges in cybersecurity is the rapidly-evolving nature of security risks. In many cases, threats are advancing faster than we can keep up with. As such, there is no one 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.

In January 2017, the US Federal Communications Commission (FCC) released a white paper calling for more regulation of cybersecurity requirements for communications networks, arguing that companies have little incentive to invest in cyber when they don't make immediate bottom line returns.

"As private actors, ISPs operate in economic environments that pressure against investments that do not directly contribute to profit," said the agency in the paper. "Protective actions taken by one ISP can be undermined by the failure of other ISPs to take similar actions. This weakens the incentive of all ISPs to invest in such protections. Cyber-accountability therefore requires a combination of market-based incentives and appropriate regulatory oversight where the market does not, or cannot, do the job effectively."

According to the paper, providers prefer to spend money to lower the cost of services to appear more competitive, often forgoing cybersecurity entirely to maintain profitability. The FCC has thus suggested that, when handing out subsidies, companies' implementation of cybersecurity best practises be considered. This movement, if implemented, could make a great difference to network security across the sector, and would be a big step forwards in basic cybersecurity.

Preparing for disaster

In the face of the rapidly-evolving cyber threats faced today, many governments are increasing their efforts to step up preparative measures and establish response procedures. The rising threat levels require a more streamlined and comprehensive programme to stay ahead of the game.

In November 2016, the German cabinet created the Mobile Incident Response Teams (MIRT) with the Federal Office for Information Security (BSI) to tackle the increased level of cyber-attacks. Similar cyber units will be formed at the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). Germany's Cyber Defence Center is set to supervise the interagency coordination and cooperation.

According to Germany's Federal Office for Constitutional Protection (BSI), the number of spam emails with malicious software in their index rose by 1,270 percent year-on-year in the first half of 2016, and around 380,000 new variants of malware are discovered every day. Meanwhile, existing anti-virus systems have lost their effectiveness. Cyber threats are growing across every sector, particularly the water and energy industries, while the top levels of government networks, notably those involved in electoral processes, are facing major cyber threats. In response, Germany plans to increase cooperation between public and private sectors. "These cyber-attacks pose such a level of threat, in that they specifically target the democratic decision-making process. If they are successful, I foresee a danger for peaceful society and for our democracy," said German Interior Minister Thomas de Maziere.

The USA is also preparing more stringent measures in the face of the rising threat. In January 2017, the US Government launched an updated National Cyber Incident Response Plan (NCIRP) from the original Presidential Policy Directive 41 issued in July 2016. The NCIRP is a strategic framework that states which stakeholders are responsible for which actions in response to a significant cyber incident. According to the NCIRP, the FBI and the Department of Justice will lead the way on threat response, the Department of Homeland Security is in charge of asset response, and the Office of the Director of National Intelligence will provide intelligence support. The affected entity response is the responsibility of the targeted entity.

Photo courtesy of Rawpixel.com/Shutterstock

"The NCIRP provides guidance to enable a coordinated whole-of-Nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure," states the new plan. "The NCIRP sets common doctrine and a strategic framework for national, sector, and individual organisation cyber operational plans."

On a similar note, January 2017 saw the Joint Committee on the National Security Strategy launch an investigation into the UK's level of preparedness on cybersecurity. The second National Cyber Security Strategy has a £1.9 billion budget to investigate the cybersecurity challenges the UK faces until 2021. The initiative was originally launched in November 2016, and is now inviting companies to present suggestions on how the UK can ensure it has watertight cybersecurity policies. Topics will include; proving information on the types of cyber threats; learning points from the first Cyber Security Strategy; the development of cybersecurity strategies; how the government should be positioned to meet threats.

"The internet has changed our daily lives almost beyond recognition from the way we communicate, to the way we trade and the way Government provides services to citizens," said Margaret Beckett MP, Chair of the Joint Committee on the National Security Strategy. "However, while the digital revolution has opened up a whole host of opportunities, it has also created new vulnerabilities. The national security implications of the leap to cyber are a matter of increasing concern."

Securing space assets

When we think about cybersecurity, most of us will consider the obvious terrestrial threats here on Earth; hacked emails, stolen identities, abuse of online banking details. For governments, those threats include everything from secure communications, financial markets, emergency services, transport networks, through to defence. Governments the world over have made significant steps in protecting their systems from future cyber-attacks, however, given our growing reliance on space-based technology, we also need to act now to keep satellite assets safe from harm.

The interception of sensitive communications via satellite is a very real worry, and one that is addressed by a number of systems today, with ever-more advanced solutions under development. In addition to the potentially deadly consequences if battlefield communications fall into undesired hands, the very high value of space assets, typically in the millions of Dollars, makes the cost of any breach by cyber terrorists extremely high. The propensity for governments to make use of commercial space assets, which often have very different security systems in place, is another challenge faced by decision-makers today.

Chatham House's think tank's *'Space, the Final Frontier for Cybersecurity?'* research report, released in September 2016, confirmed that satellite security needs more attention: "The vulnerability of satellites and other space assets to cyber-attack is often overlooked in wider discussions of cyber threats to critical national infrastructure. This is a significant failing, given society's substantial and ever increasing reliance on satellite technologies for navigation, communications, remote sensing, monitoring and the myriad associated applications. Vulnerabilities at the junction of space-based or space-derived capability with cybersecurity cause major national, regional and international security concerns, yet are going unaddressed, apart from in some 'high end' space-based systems. Analysing the intersection between cyber and space security is essential to understanding this non-traditional, evolving security threat."

Securing space-based communications is top of the agenda for many, and the Chinese Academy of Sciences (CAS) is looking to do just that with Quantum Experiments at Space Scale (QUESS), the world's first quantum communication satellite. QUESS contains a quantum key communicator, processing unit, laser communicator, and a quantum entanglement source to transmit quantum keys to Earth. The quantum entanglement principle, where two particles are fused into complementary quantum states, is used to provide hack-proof communications on the basis that quantum photons cannot be separated or duplicated without detection.

In January 2017, QUESS became operational after months of in-orbit testing. Launched in August 2016, QUESS was designed to provide 'hack-proof' communications to enable China to provide high-level communication security support to islands in the South China Sea, Chinese embassies and consulates in foreign countries, and naval vessels.

Pan Jianyu, Chief Engineer of the project, stated that the research team has begun to carry out experiments transmitting hack-proof messages to two ground stations separated by 1,200km. The first mission will demonstrate a quantum key distribution i.e. the encoding and sharing of a secret cryptographic key using the quantum properties of photons, between a ground station in Beijing and QUESS, and between Vienna and QUESS. Next, the tests will show whether a quantum key can be established between Beijing and Vienna using the satellite as a relay. The second mission will perform a long-distance entanglement distribution over 1,000km. One photon from an entangled pair will be beamed to a station in Delingha, Tibet, and the other to a station in Lijiang or Nanshan, which are some 1,200km apart.

Pan Jian-Wei, Chief Engineer of the project, stated: "In principle, quantum entanglement can exist for any distance. But we want to see if there is some physical limit. People ask whether there is some sort of boundary between the classical world and the quantum world: We hope to build some sort of macroscopic system in which we can show that the quantum phenomena can still exist."

Looking to the future

Cybersecurity is clearly going to be a major part of our lives for many years to come. It's essential that governments stay on top of the threat of cyber-attacks for the safe-keeping of their nation with new, concise policies that cover every critical sector. Public-private sector partnerships have a big role to play going forwards, while information sharing and enhanced cooperation between entities will have a significant positive impact on cybersecurity systems. New products promising next-generation protection age rapidly compared to the ever-evolving threats, but innovative solutions like the QUESS quantum communications satellite could be real game-changers in the future.

It's clear that, going forwards, the security of our private information, both individual and state-wide, will be under greater threat than ever before. What's not yet apparent is whether we'll be able to combat those threats effectively. **GMC**

Photo courtesy Billion Photos/Shutterstock

Photo courtesy Den Rise/Shutterstock

If this is **your office...**

these are **your HPAs.**

Superlinear® TWTAs
LEFT: 2.5 kW X-band
CENTER: 750 W Ku-band TWTA

Solid State BUCs
RIGHT: 160 W peak Ka-band GaN BUC

Warfighters shouldn't have to fight against their equipment.

That's why CPI amplifiers feature better efficiency and unmatched reliability even in the harshest of climates, keeping you connected anywhere at any time.

CPI offers:

- Better efficiency
- High reliability
- Rugged designs
- TWT, solid state and klystron technology
- Linearizer, BUC, and integral switch control options
- More than 20 service centers worldwide
- 24/7 technical support

For more information, please visit **www.cpii.com/satcom**, contact your local sales representative, or call us at **+1 (650) 846-3803.**

HPAS FOR MILITARY APPLICATIONS

- Up to 700 W Ka-band TWTAs
- SuperLinear® TWTAs in Ku- and Ka-band, delivering 25 to 540 watts of linear power
- C- and Ku-band HPAs for troposcatter applications
- 400 to 750 W C-, X-, and Ku-band indoor and outdoor TWTAs
- 2500 W SuperLinear® and CW X-band TWTAs
- X-, Ka- and Ku-band GaN BUCs

Download our new app!
Search: CPI Satcom

Download on the App Store

GET IT ON Google Play

CPI
Communications & Power Industries

satcom products