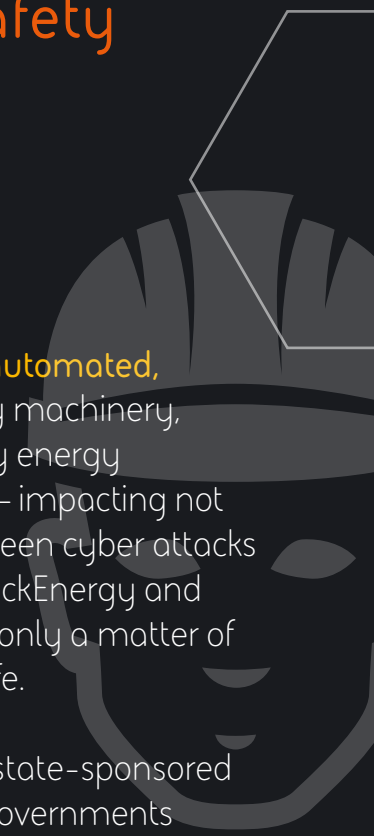
BAE SYSTEMS

2020 Predictions

Cyber concerns become safety concerns

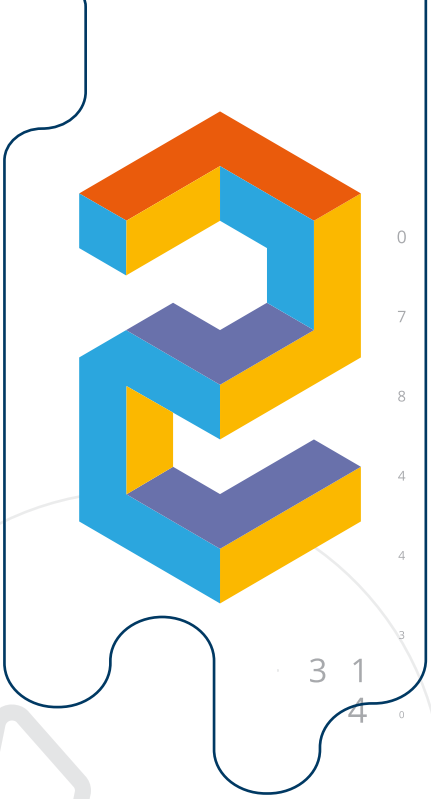


Human safety has become dependent on automated, connected, cyber-physical systems. Factory machinery, medical devices, autonomous vehicles or city energy distribution going down could be disastrous – impacting not just costs but human life. We have already seen cyber attacks disrupt access to basic resources with the BlackEnergy and Industroyer malware in 2015 and 2016 – it is only a matter of time until we see a cyber threat to human life.

If safety is compromised by an attributable state-sponsored cyber attack, this will draw the attention of governments and international law – **the Secretary General of NATO Jens Stoltenberg has already made it clear that a cyber operation could trigger Article 5,** and adversaries may choose 2020 to test that commitment.

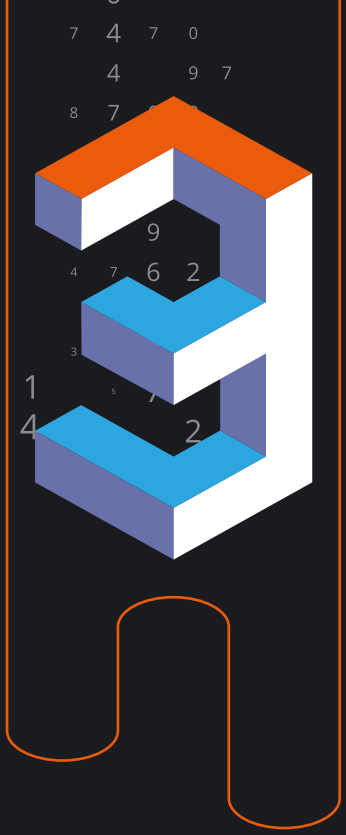
As cyber threat actors focus more on targeting industrial equipment and critical infrastructure including emerging 5G technology, there needs to be a big shift in safety mentality to include cyber security, or we anticipate civilians will suffer the physical consequences of cyber attack in 2020.

As criminal cyber operations get more funding and more sophisticated, the **more financial related attacks will arise**



Previously we've largely seen cyber criminals attack consumers, business accounts, and banks. **In 2020 criminals will delve deeper into the financial ecosystem,** targeting payroll services, interbank networks, Fintechs and Open Banking.

These high-end cyber criminal groups are funded in part by their global money-stealing cyber operations, by large ransomware payouts including from government and critical infrastructure targets, and even by some of the state-sponsored cyber threat groups that we track, who increasingly purchase tools and victims from cyber criminals. **With more funding channels and better toolsets, there is no sign of cyber criminal activity dropping.**



Cyber insurance policy holes lead to legal action

Until recently, cyber security risks have been absent from insurance documents, with some insurers refusing to pay out after a cyber attack under the "acts of war" exemption.

Cyber insurance products are emerging but still need to tackle the array of possible outcomes: what costs would arise from a denial-of-service ransomware attack, versus theft of personal data, versus a threat to leak intellectual property? **What if the attack is made possible by a cyber vulnerability that the organisation should have known about and mitigated already?**

As it becomes clearer what a cyber attack actually costs, and who has insurance, criminals will adapt their targeting and ransom demands accordingly.

Social media companies invest in bigger compliance teams

Social media giants operating globally often appear to have an "open to all" philosophy about sharing content online, however they still have to comply with individual laws of the countries in which they operate.

Governments have different stances and priorities when it comes to free speech, violent or extremist content, online abuse, political campaigning, and fake news. Well-planned misinformation campaigns and hyper-realistic "deep fake" video technology further complicate the challenge of establishing which content to block.

The desire by governments to clamp down on parts of the vast and complex online content will make it harder for social media platforms to keep compliant with many different laws across the world. This can be compared to the banking sector, where a global bank investigating a fraud or money-laundering operation needs large compliance departments to address the challenges of operating with different national laws and regulations.

Rise of a new international cyber-power

The internet and computing technology have been democratising forces since their inception, and the barriers to entry in tech are lower than ever. **2020 may be the year a new international power takes the world stage** – all because of their cyber capability. A previously smaller or sidelined country could establish offensive cyber capabilities that would put the international community on alert.

The best wisdom in the intelligence community tells us to stop fighting the last war and look to what the next one will be. A protracted period of back-and-forth cyber attacks could bring the world to a sudden stop. As more countries and militaries begin to realise the importance of cyber defence, **bad actors will turn to higher-tech threats to get what they want.** In 2020, we may hear less about a nuclear option, and more about a cyber option. In the wrong hands, it could be just as threatening.

Summary

Clearly, 2019 will continue to have some **significant cyber security hurdles,** with the shortage of cyber security professionals among them. The amount of complexity in cyber security systems continues to make staying ahead of hackers difficult and time consuming.

This is the opportune moment for businesses to revisit their cyber security plans to **make sure they have the right mix of technology** to detect cyber attacks and the right people to defend against them.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/compliance

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai