



Looking Back  
to **Spring Forward**

BAE Systems 2019 Cyber Threat Predictions



# Our predictions for 2019

In businesses around the world, 2018 showed us that cyber security vulnerabilities continue to grow and evolve. As more sophisticated cyber criminals join the ranks, more malware is being launched than ever before. It is estimated that approximately **300,000 new malware samples** are generated per day. The business impact and complexity of managing cyber security is increasing dramatically, as is the need to justify cyber security investments and provide reporting relevant to the business to prove the value of those investments.

Advances in technology like **artificial intelligence** and **machine learning** accelerate the pace of new, data-driven solutions, but this can be a dual-edged sword as **bad actors** can leverage them into more sophisticated attacks on companies that are just trying to stay abreast of current threats. From **malicious chatbots** to the **explosion of web apps** making their way into corporate networks, 2019 will likely continue to be challenging for cyber security teams.

At BAE Systems, we have over 40 years of experience in securing the assets of governments, nation states and businesses. Our vast reach gives us a unique perspective on the state of cyber security. With that in mind, **Adrian Nish, BAE Systems Head of Threat Intelligence** offers his predictions for 2019.



# Bank heists move to real time

Given the record number of cyber heists in 2018, it is likely bank networks will continue to be in the crosshairs of financially motivated threat groups in 2019. However, there will be changes in how these groups attempt to move money from bank systems to their own hands. Many attacks over recent years have focused on international interbank payment systems. These have a major disadvantage for criminals though, in that there is a delay of 24-48 hours before the funds are settled and available to be moved. This time window allows the authorities time to catch up following an attack and freeze the funds.

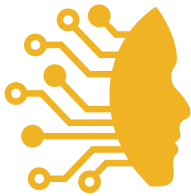
In 2019 we anticipate attackers will shift to targeting systems that allow real-time settlement of funds – meaning that money can be moved through a network of accounts more quickly and ultimately laundered successfully. This will present a challenge for the community in terms of the speed of response and international co-operation.



# The death of the password

How many times over the past year have you had to click a 'Forgot Password' link? And was that more than the previous year? For all but the geniuses among us, the challenge of remembering individual passwords for dozens of websites and apps is becoming too much to handle. Add to this the fact that more vendors are following 'best practice' and forcing use of special characters, increased length, regular password changes; and the task quickly becomes impossible.

Security engineers have long had it in for passwords, and leading tech firms have begun to adopt smarter, more friction-free alternatives. A 'survival-of-the-fastest' rule exists for online services, and those presenting a login screen hurdle will find their usage declining as leaders choose new authentication technologies. Could 2019 be the year that turns the tide on the scourge of passwords?



# Anti-AI activists attack

Advances in machine learning and automation are set to bring continued benefits to businesses and consumers alike. However, this is not without costs and risks. Displacement of workers will lead to social issues; a proliferation of data collection will create privacy and security concerns; and there will be worries that the robots are making too many decisions or taking over (Hollywood has been forewarning us of this for decades...).

In 2019 we may see the emergence of activist groups concerned with the potential for an AI revolution and the negative impacts this may have. Such groups could begin to deploy tactics to counter robotic systems and AI. For example, putting stickers on road signs to trick sensors in autonomous vehicles resulting in mistakes and potentially even accidents.





# Bitcoin crashes

The value of anything is only whatever someone else is willing to pay for it. For Bitcoin in 2019 that may well be close to zero. The Bitcoin bubble is bursting, and a 40% drop in recent months may be foreshadowing even further falls to come next year. Although there is still promise that crypto-currency could yield benefits for consumers, for example in areas such as speed of transaction and global portability, the recent volatility will scare off both investors and potential corporate users. Without mainstream adoption, the hope of stabilisation will diminish and those who've previously invested will look to sell while they can. 2019 could be a year of reckoning for Bitcoin, but it need not spell the end of crypto-currency generally.



# Testing times for regulations



The Panama Papers and subsequent revelations have resulted in a greater requirement for regulated industries to Know Your Customer (KYC) and establish Ultimate Beneficial Owner (UBO). 2019 will further put pressure on the sector around KYC, but will also see extra constraints due to GDPR. UBO requirements ask for more data to be analysed, but GDPR asks for proportionate data to be analysed. The regulations are at odds with each other in regards to financial crime prevention and we anticipate this will cause more challenges for organisations required to comply with both. This will likely result in test cases to establish how organisations interpret the conflicting needs and potentially even changes in regulations as lessons are learned.



# 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](mailto:learn@baesystems.com) | W: [baesystems.com/businessdefence](https://baesystems.com/businessdefence)

 [linkedin.com/company/baesystemsai](https://linkedin.com/company/baesystemsai)

 [twitter.com/baesystems\\_ai](https://twitter.com/baesystems_ai)

Copyright © BAE Systems plc 2018. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.