TOBBY SIMON

Founder and Chairman of Synergia

Patrick Nicolet, CEO of Linebreak Ltd., former Group Chief Technology Officer of Capgemini

All this is about exploiting data and of course, this data needs to be protected. So what do we do in cybersecurity?

Tobby Simon, Founder and Chairman of Synergia

Thank you, Patrick, and thank you Thierry for this opportunity to speak at the World Policy Conference.

We live in very interesting times and the current security architecture has been compounded by multiple conflicts, contestation in space and the quick adaptation of emerging and advanced technologies.

In the allotted time, I will speak about three distinct things.

The first will be the premise, second, the threats, third, the strategy as we see it.

I will also briefly mention about quantum technology, less on quantum computing which is the remit of a second speaker. Finally, I will share some examples of AI and Cyber and what it bodes for the future.

Let me set out the premise. First, we can all agree that there are no airgaps in cybersecurity, be it perimeter, cloud, space or edge. Two, the surface area of cyber vulnerability has expanded many folds with the adoption of IoTs and sensors. This is particularly true because we are living in a world where most of our critical infrastructures are connected. Three, encryption is everywhere and securing our encryption is key to our digital future or success. Today, we are more an encryption economy, and an example to consider would be digital signatures. Everything we validate digitally is based on digital signatures and if there is a vulnerability on that, you can imagine how that could compromise our future.

Second, I will briefly allude to the threats. Global trends in cryptography are heavily compromised as powerful algorithms like Shor's and Grover's use equally powerful computers that can crack any encryption standard. They do that with quantum simulators, which are very powerful computers that can compromise encryption. When it comes to quantum computers, we all knew the advent of Y2K, it was known in advance as Jan 1st, 2000, but nobody knows with certainty when quantum computing will arrive. Truly it is managing the unknown.

Third, the majority of encrypted web data relies on an encryption standard called RSA 2048. A quantum computer with 4099 cubits will be able to break the encryptions it in a few minutes.

We do not see such a possibility extending beyond 2028 -2030 or it may already have happened. Systems using today's cryptography for long-term authentication is at risk. For example, consider the health data and the possibility that they have been compromised. Many hospitals being hacked because their data has a very long tail. Cryptography based on mathematical algorithms is vulnerable to brute force attack. The grid will likely become the first target in the line of attack when nations are in conflict. There could be other compelling economic reasons too. This includes national defense systems, critical infrastructures including utilities like power, financial institutions, healthcare, military - they have become critical infrastructures when we speak of comprehensive national security.

The strategy, which are being employed now by hackers is twofold: First of which is hack now, weaponize now. If you have the algorithm and cryptography to break these encryptions, you weaponize it now. The second option is to hack now, store it and weaponize it later when you have the ability to beak the encryption.

Fundamentally, what we are trying to propose now is to move from an encryption based on mathematics to quantum physics, which according to fundamental science is much more difficult to crack. This premise rests on three principles, one of which is Heisenberg's Principle of Uncertainty, which makes it possible to identify eavesdropping. In fact the wave collapses as soon as there is an intrusion. Second is the no-cloning theorem which prohibits copying of data from quantum states. The third is the inequality principle which prevents implanted attacks on physical systems.

I will not go into quantum computing but let me talk about quantum technology, which arises from the second quantum revolution. Incidentally, the first quantum revolution included, nuclear, semiconductors and lasers. The second is more characterized by manipulating of individual quantum systems, for example, eavesdropping using quantum key distribution, quantum computing breaking the RSA code.

I will now allude to AI and cyber. AI systems will be one of the go-to adversarial attack vector from any domain where AI augments action. That means the moment you use AI there is a vulnerability, it is a like a boomerang, it can possibly ping you back. The attack involves data poisoning and data manipulation, thereby rendering AI very ineffective. For example, let me give you a conflict scenario, let us say the field used in AI is supercharged Intel, ISR. The AI use case would be object detection, which is asset, person and reference, and the AI attack would be extraction and evasion. If you look at what the Russian's were able to do with their military fields in this current conflict, you will see a lot of this exploitation happening and mark most of the places they had kept their aircraft.

The combination of AI used with HAPS (High Altitude Pseudo Satellites), using satellites would be a little more challenging but HAPS that are operate at a much lower altitude could become aerial data centers. In future, when we are moving into a theatre of autonomous warfare, we will be using more of HAPS, which will ensure quick communication to people in the field. Second, with the advent of human enhancement technology, cybernetically enhanced human beings with implants in their bodies are able to connect to a HAPS and take decisions much faster than if they were calling a command center.

Finally, looking to the future there are AI-based neural systems. You have AI and quantum but the challenge of AI or the success of building quantum encryption is based on how much complexity you can achieve. With AI you can increase this complexity using a technology we call ciphertext. Currently the highest standard is about 2^{256} but with AI-based neural systems you can increase the complexity of ciphertext to about $2^{2.6\text{million}}$. That is what the future of AI encryption will look like, there are pluses and minuses but this is how I see the technology evolving.

In conclusion I have emphasized the military part of it more because we believe that defense organizations are likely the most early adopters of most advanced technologies and having them validate the technology is a more pragmatic way to approach the general market.

Patrick Nicolet

Thank you, Tobby. That is a good point connecting to the story Kazuto mentioned about the need for distinctive policies. There are two points I take from this, when it comes to AI and cybersecurity you described complex systems and the more complex they are the more they increase the attack surface. Notably, what you have seen from Ameena, and what Tobby explained, a lot of identities will be created for all these machines. One of the major points in cybersecurity is managing identities and access to systems based on that, so that is a big complexity. Then, you also use AI for the attack, which there is an attempt to neutralize and unfortunately the parallelism is not yet in place so we have some challenging times ahead of us. Thank you for this overview, Tobby.