

Understanding the Relationship Between AI and Cybersecurity

March 22, 2018 | By [David Strom](#)



Thinkstock

The first thing many of us think about when it comes to the future relationship between artificial intelligence (AI) and cybersecurity is Skynet—the fictional neural net-based group mind from the “Terminator” movie franchise. But at least one security professional (with a somewhat rosier view) suggested that AI must be understood across a broader landscape, regarding how it will influence cybersecurity and how IT can use AI to plan for future security technology purchases.

Earlier this year, [Dudu Mimran](#), chief technology officer (CTO) at Telekom Innovation Laboratories in Israel, discussed the relationship between [AI and cybersecurity](#) in a speech and subsequent [blog post](#) for the Organisation for Economic Co-operation and Development (OECD)

Forum 2018. I caught up with Mimran at his office in Beersheba, Israel for an interview, which we continued later over email.

The Short- and Long-Term Forecast for AI and Cybersecurity

“While the threat of cyberattacks powered by AI is increasingly likely, I am less concerned in the short- and midterm about machines making up their minds and being able to harm people,” Mimran said. “Our lives are becoming more and more dependent on technology, and this will be exploited by adversaries much before we have conscious machines. Nevertheless, today most of attackers’ goals can be attained without the sophistication of AI, and that is why we don’t see a big new wave of these kinds of attacks.”

In his OECD speech, he mentioned four time horizons:

- a. Short-term hyper-personalization, where algorithms are getting to know us better than we know ourselves
- b. Medium-term disruptions based on various focused automation efforts
- c. Long-term pervasive autonomous machines, such as driverless cars
- d. Long-term situations, such as malicious, Skynet-type scenarios

Applying AI to Malware Attribution

One of the most significant potential benefits of AI technology is [malware attribution](#). If you know your attacker and can respond quickly, according to Mimran, “the chances you will be hitting back your true adversary are higher if you can react in real time.”

However, he noted in his OECD speech that attribution “suffers from underinvestment because it lacks commercial viability.” This is a well-known problem because researchers have to check so many variables, including the written noncoding language of malware, the used cultural or political references, and what code fragments mimic existing malware structures.

Mimran suggested two ways in which policymakers can improve attribution. The first is by supporting and building a joint global intelligence network that can track threats across different geographies and includes both business and government researchers. The second suggestion is to fund ongoing research to help improve attribution while preserving [data privacy](#).

“Attribution is a distributed problem, spanning across different technology stacks, systems, and organizations, and these central entities can help weave such a thread,” Mimran said. He said he is optimistic—especially about new security startups focused on these collaboration ideas and an initiative with the largest European banks to collaborate on shared threat intelligence.

Preserving Data Privacy in the Age of AI

The data privacy element is an important consideration. As Mimran [wrote last year](#), “High amounts of personal data distributed across different vendors residing on their central systems can increase our exposure and create green field opportunities for attackers to abuse and exploit us in unimaginable ways.”

One solution to the privacy issue is some form of blockchain-based innovation. Mimran mentioned ForgeRock and others that have recently been funded. “The challenge for these companies is integration with the rest of the world,” he said. “Identity is mostly embedded deep into online services and products, and creating an external neutral entity that will

enable the same smooth experience with all the services out there is a significant challenge.”

Separating the Wheat From the Chaff

These technologies also have applications for other cyberdefense tactics. “We do see an initial effort of AI used as an automation tool in the security operations center [SOC], but these are just preliminary,” Mimran said.

However, it is important to be cautious — particularly when vendors try to oversell their tools and claim they are AI-based. [CSO Online](#) emphasized the importance of delineating between products that have rules-based detection engines and ones that leverage true AI, since “many vendors with hundreds of rules feel they have accomplished some sort of near version of AI,” and merely verifying an existing malware signature constitutes not AI but mere pattern matching.

Mimran also mentioned the growing threat of [Internet of Things \(IoT\) botnets](#). “The problem of IoT botnets touches on many loose ends in the way technology is built today, and there is no silver bullet for that. The best way to tackle botnets is when cooperation emerges between the hosts of the bots, along with the communication or services provider which tunnels the bots’ traffic and law enforcement,” he said.

Shifting Away From a Skynet-Esque Future

The [rise of AI](#) certainly does further complicate the threat landscape, but organizations that recognize the importance of threat intelligence sharing, malware attribution, and data privacy can stay ahead of cybercriminals aiming to exploit or leverage the technology for nefarious purposes. Ultimately, security teams that understand AI properly — and invest accordingly — will be well-equipped to unlock its many

cybersecurity benefits before threat actors make any headway toward creating a malicious, Skynet-style dystopia.

<https://securityintelligence.com/author/david-strom/>

David Strom

Security Evangelist

- Follow David Strom on Twitter
- David Strom's Website
- Follow David Strom on LinkedIn

David is an award-winning writer, speaker, editor, video blogger, and online communications professional who also advises numerous startup and well-established technology ventures. He began his career as an in-house IT analyst and has founded numerous technology print and online publications, such as editor-in-chief of Network Computing magazine and as part of the launch team of PC Week's Connectivity section. David has written two books and spoken around the world at various conferences and been on national radio and television talking about network technologies. He continues to build websites and publish articles on a wide variety of technology topics geared towards networking, security, channel, PC enthusiasts, OEMs, and consumers. In addition to these activities, he consults to vendors and evaluates emerging technologies, products, strategies, and trends to help position and improve their technology products.