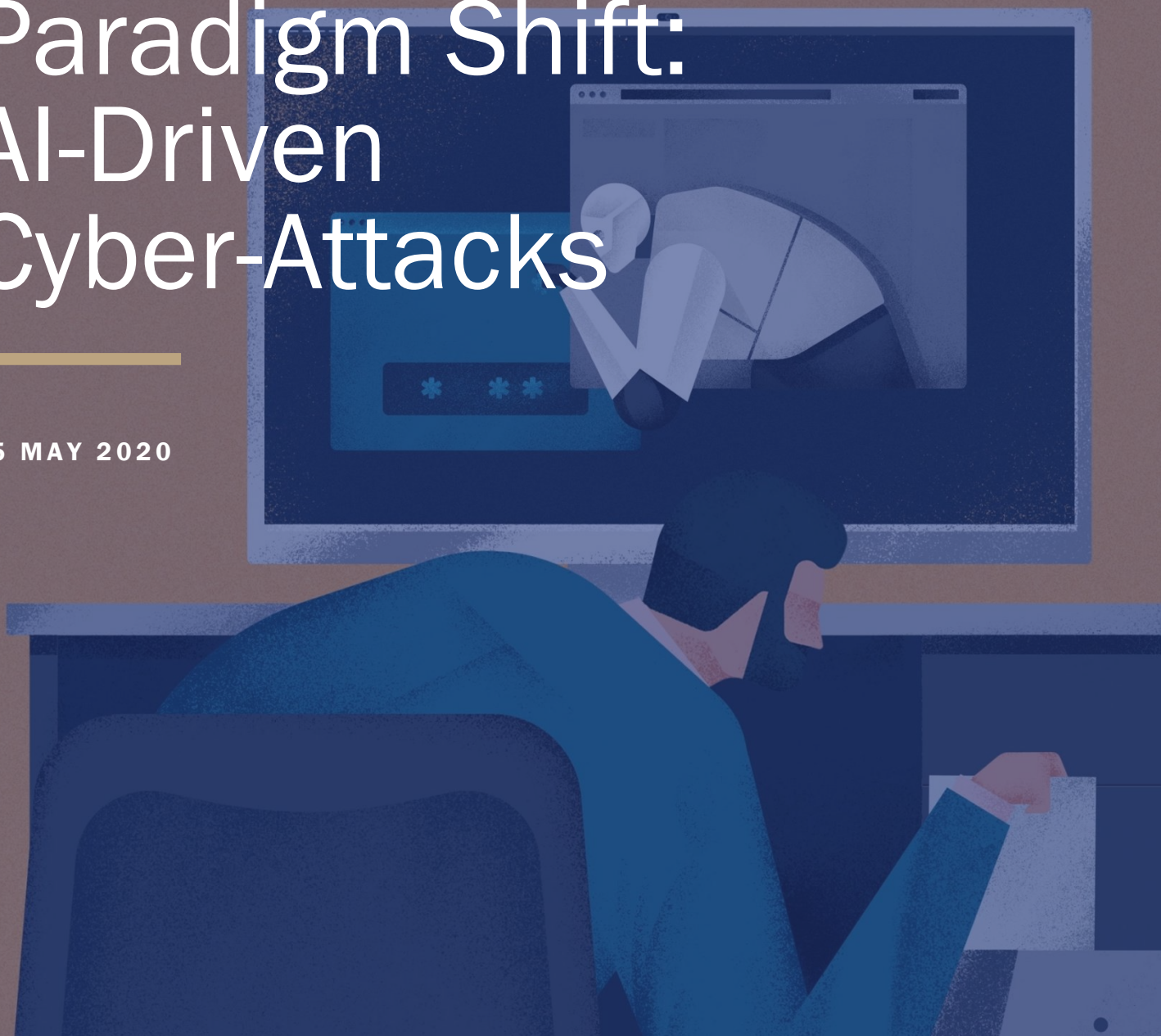
GIC

THINKSPACE

PERSPECTIVES ON

The Next Paradigm Shift: AI-Driven Cyber-Attacks



15 MAY 2020

As Artificial Intelligence (AI) continues to transform global industries, it is also adopted by cyber criminals to strengthen and scale up cyber-attacks. Nicole Eagan, CEO of Darktrace, a leading AI cyber defence company with over 2,500 customers globally, discussed cybersecurity trends at the Bridge Forum 2019, a unique experience co-created by GIC and the Singapore Economic Development Board to guide businesses through technology disruption. Below is a compilation of the key takeaways from her sharing, including today's landscape, case studies and best practices on muzzling threats.

Cyberwarfare is becoming a battle of algorithm against algorithm. The majority of cyber-attacks today are still human-generated, but what lies ahead are increasingly deadly assaults by attackers using AI. Cyberwarfare driven by AI will move at machine speed, outstripping the ability of human defenders to respond.

HOW QUICKLY DO THESE ATTACKS TAKE PLACE?

The time taken to get a cup of coffee, or to chat with your desktop neighbour. That is the amount of time needed for a cyber-attack to take place. As networks compete with each other, they will continue to become smarter, more powerful, and accelerate constantly. Human teams working to protect their organizations and data from cyber-attacks will need the strength and sophistication of AI to stand any chance of gaining the upper hand.

THE THREAT OF CYBERWARFARE

Our most advanced industries are well ahead on the technology curve, and pay close attention to the threat of cyber-attacks. Their boards of directors recognise the danger and the C-suites are engaged. Yet, breaches continue to happen. There are two reasons for this:

1. Cyber-attacks are ever-evolving. Today, a very large global crime ring exists, one that has links to nation states and that is infiltrating into cloud systems and corporate networks. This is a new, different level of threat, well beyond what companies were contending with a decade ago.

2. Companies are evolving their underlying business models, moving rapidly into digital transformation, AI and the cloud. What happens is that every time a company connects more devices and more customers connect with a company's network, the "attack surface" is increased. Coupled by the

urgency of digital transformation, companies can sometimes overlook building in the necessary security measures from the start. This opens them up to vulnerabilities, which hackers can exploit and prowl unnoticed for long periods before or as they wreak havoc.

TAKING INSPIRATION FROM THE HUMAN BODY

The increasing speed and sophistication of cyber-attacks requires a new approach to cyber defence. ***Inspiration is coming from an unlikely but highly instructive place — the human body,*** and its extraordinary ability to detect and defeat external threats. Our immune system is constantly under attack from viruses and bacteria, and has over time evolved an innate sense of self to understand what belongs within the body and what the foreign bodies are, and most importantly, how to mount a precise and rapid response to harmful, invasive elements.

Cyber defence with AI works in pretty much the same way. It analyses thousands of data features across a company's network, from email and cloud to applications such as Office and Salesforce in order to build a "pattern of life", with an in-depth understanding of the specific and unique complexities of every user and device connected to that network. Once it understands a network's regular life pattern, intrusions of any kind are more readily identified and defeated.

CASE STUDIES: OMNIPRESENT THREATS AND THE USE OF AI

Nicole shared three case studies that demonstrated the breadth of vulnerabilities in corporate networks today, and how AI can defeat them.

1. *Fish tank in casino lobby*
   Hackers infiltrated the thermostat in a high-end fish tank located as an attraction in a casino lobby made vulnerable through its individual VPN. The hackers' intent was to upload personal data on the casino's high rollers to a private cloud in Finland. The casino's legacy security systems missed the intrusion, but AI found it by identifying both the fish tank's data upload and its transfer to a private cloud in Finland as system outliers.

2. *Mobile banking app*
   A developer enhancing the bank's mobile app accidentally changed its security protocols such that its previously encrypted data would now travel unencrypted. Although unintentional, the error could have exposed customer data to attackers. AI detected the anomaly of unencrypted data transfer over a File Transfer Protocol (FTP) port in less than two seconds and a patch fixing the misconfiguration was quickly put in place.

3. *CCTV at a financial services firm*
   Hackers entered an Internet-connected CCTV system at a financial services company in Japan, attempting to port private video footage to an offsite facility for analysis, and potentially compromising content from the CEO's office, executive conference rooms, whiteboards, and more. AI detected the anomaly of data moving to and from the CCTV server, and surgically blocked the data transfer, while sustaining normal camera functions.

BEST PRACTICES IN ADOPTING AI FOR CYBERSECURITY

The overwhelming reality of cyber-attacks today is that they can come from anywhere, attack any point of entry at any time, and infiltrate a network in seconds. For AI to achieve its full potential in fighting cyberwarfare, best practices are key. Our key lessons are:

Ensure visibility: No one wants to rely on a black box, without any understanding of what goes on inside the box — that is what makes humans nervous about AI. For people to trust AI, it needs to be visible. The most human-friendly AI solutions deploy 3D visual guides with graphic elements to depict the cloud and illustrate how data flows through the network.

Make it mobile: Cyber-attacks are not desk-bound, so the protections against them cannot be either. AI defenses need to be mobile, with apps, real-time alerts, and flexible decision trees that enable IT teams to evaluate and respond quickly from any location.

Know yourself: Like the body's own finely-tuned immune system, AI works best when it is grounded in comprehensive understanding of all aspects of its physical operations. For AI to shield from cyber-attacks fully it first must be deployed fully, and not introduced piecemeal.

Without a doubt, AI is necessary if we want to win this cyberwar. Human teams that battle cyber-attacks without AI will more often than not be overwhelmed. In the war of algorithm against algorithm, AI can and should be on our side, slowing cyber-attacks and, ideally, stopping them in their tracks.