Viktor Prokopenya: Navigating the Challenges of Digital Warfare

The growing threat of Russian cyber-attacks on Ukraine has highlighted the urgent need to address this warfare in the modern world. With an alarming history of targeted attacks on civilian infrastructure and recent incidents affecting whole nations, the implications of these cyber assaults cannot be ignored.

Viktor Prokopenya suggests looking at Ukraine's experience in cyber warfare. As a renowned entrepreneur and founder of Capital.com, Prokopenya has had a firsthand experience with the devastating effects of Russian cyber-attacks. His company in London was subjected to a massive "distributed denial of service" attack after Prokopenya announced it would cease operations in Russia to protest the invasion of Ukraine and donate £1m to Ukrainian charities.

Note: A "distributed denial of service" or DDoS attack involves numerous computers worldwide overwhelming a company's website with requests, aiming to overwork it and potentially cause a shutdown.

Ukraine's Battleground: A History of Russian Cyber Aggression

First, let's turn to history. Throughout the years, Ukraine has faced a series of relentless cyber-attacks orchestrated by Russian actors. The extent of these attacks underscores the severity of the threat. Notable instances include:

Ukraine's Battleground: A History of Russian Cyber Aggression

First, let's turn to history. Throughout the years, Ukraine has faced a series of relentless cyber-attacks orchestrated by Russian actors. The extent of these attacks underscores the severity of the threat. Notable instances include:

Legal experts and researchers have previously made the case for the ICC to prosecute Russian cyberattacks. But now Ukrainian officials, as a sovereign government, have taken the initiative by sharing information about Russian cyber-attacks with the International Criminal Court (ICC), urging investigations into potential war crimes. The interpretation of existing laws, such as Article 8 of the Rome Statute, should encompass the destructive potential of cyber-attacks and their parallel with physical destruction. The ICC must adapt to the complexities of 21st-century "hybrid" warfare.

In 2022, the British government unveiled a Cyber Security Strategy to tackle cybercrime. However, Victor Prokopenya stresses that there are few proposals in the document for legislation that is badly needed to improve cybersecurity. Updating the Computer Misuse Act to combat emerging cyber-crimes, addressing data protection and online child safety, protecting critical infrastructure, and safeguarding intellectual property rights are paramount to ensuring national security in the digital era.

Ukraine’s Resilience: Lessons to Learn

In the face of relentless cyber aggression, Ukraine has displayed remarkable resilience. Viktor Prokopenya highlights the creation of a volunteer cyber force as a prime example of Ukraine’s innovative response.

An important point is that their activities are supported and to some extent sanctioned by the Ukrainian government, although such involvement is officially denied. The department that created the telegram team for the IT Army of Ukraine grouping is supervised by the Deputy Prime Minister and Minister for Innovation, Development of Education, Science and Technology of Ukraine, Mikhail Fedorov.

The most interesting Ukrainian cyberattack cases:

- An attack on Honest Mark, Russia’s mandatory product labelling system. Using a DDoS attack, hackers found a way to disable the service, resulting in significant economic losses for Russia.
- Over 800 Russian websites, including Roscosmos, were attacked, with congratulatory messages posted for Ukrainian Constitution Day.
- The IT Army targeted the Moscow Stock Exchange and Sberbank, rendering the websites inaccessible in just five minutes.
- Hackers invaded Russian radio systems, transmitting false air-raid alarms and the need to take shelter in bomb shelters.
- Collaboration with Anonymous: The group collaborated with Anonymous to cause a traffic jam in Moscow by attacking Yandex Taxi’s systems.

As Viktor Prokopenya says, these responses serve as a model for other nations. Enhanced proactive defenses, innovative approaches to cybersecurity, and collaboration between public and private sectors are strategies that can be used by countries to create a secure digital future resistant to cyber threats.

About Viktor Prokopenya

Viktor Prokopenya is a British technology entrepreneur and investor originally from Belarus. Founder of investment company VP Capital. He contributed to the adoption of the Decree on Digital Economy in Belarus in 2017. Still, despite this, Viktor Prokopenya was forced out of Belarus during the policies pursued by Alexander Lukashenko.