The New Iron Curtain is Digital: How Russia Weaponized TikTok in Romania and DDoS Attacks in Estonia

Since Russia's full-scale invasion began in February 2022, the Russo-Ukrainian war has continuously evolved, with a significant portion of the conflict now being fought from a distance. Information technology (IT) systems have become an increasingly crucial part of government and military infrastructure on both sides. As a result, they are frequently targeted with the aim of disrupting coordination and operational efforts. This so-called "non-kinetic battlefield" has essentially transformed the traditional war into a hybrid one, with two battles being fought in parallel. Oftentimes, cyber-attacks are coordinated with physical ones: IT infrastructure supporting logistics and communication is being disturbed in order to increase the chance of a successful assault. Part of the hybrid conflict is also spilling over to the countries supporting Ukraine, with nations across Europe facing increased attempts from hackers to incapacitate their information systems: Spain, Belgium, and the Netherlands facing Distributed Denial-of-Service (DDoS) attacks, conversations by German military personnel being leaked, and the examples go on.

Among the nations facing the wrath of Russia's electronic warfare are Estonia and Romania. Whereas Estonia is facing DDoS attacks across their digital government infrastructure, Romania has suffered from attempts to destabilize the country by influencing the presidential election results through social media, as well as attempts to tamper with the electronic voting system. How are these two nations adapting to the growing threat of digital interference in their national security, and what lessons can be drawn from their responses to Russia's cyber tactics?

Estonia's Journey Towards Becoming a Digital Fortress

Estonia's post-Soviet history has positioned it on the front line of the Russian Federation's influence campaigns. These operations aim to sway public opinion within the former Soviet state through a combination of disinformation and hostile cyber activity. The 2007 cyber-attacks which lasted for several weeks are a prime example of this strategy. Precipitated by the controversial removal of a memorial to the Soviet Red Army, the attacks consisted of DDoS attacks which put a great amount of strain on the Estonian national IT infrastructure, including government portals and the banking

industry. The event demonstrates a clear link between political decisions and retaliatory electronic warfare.

The attacks served as a catalyst for Estonia to significantly invest in its national cybersecurity. This strategic focus has transformed the nation into a global leader in cyber defence, as shown by its position in the highest performance tier of the ITU Global Cybersecurity Index for 2024. The resilience of Estonia's cybersecurity was recently demonstrated against a new wave of attacks by two politically-motivated Russian hacker groups. Despite a sharp increase in activity - impactful incidents nearly doubled from 3,314 in 2023 to 6,515 in 2024 - the resulting damage was minimal, with no attacks causing severe disruption to any electronic services.

Estonia also successfully defended against a similar attack which took place in 2022, when multiple DDoS attacks were launched by the Russian hacker group "Killnet" against a series of websites owned by the public and private sectors. These attacks came alongside fake news from Russian media suggesting that Soviet war graves were being destroyed by the Estonian government, angering the ethnic Russians in the country. This has, once again, happened after Estonia removed Soviet-era monuments.

The Algorithmic Battle for Romania's Ballot Box

In today's age, social media has become a platform where political candidates can connect with their supporters in a more personal, unmediated way. Platforms like TikTok offer a significant departure from the one-way broadcasts of traditional media, such as television advertisements or campaign banners. They provide a venue for candidates to share more authentic and interactive content, fostering a level of voter engagement that is difficult to achieve through conventional materials. The most recent controversy regarding the Romanian elections revolve around Calin Georgescu, who secured a remarkable 22.94% of the vote in the first round in spite of a pre-election popularity rating of less than 1% just one month before. He successfully leveraged TikTok's algorithm to his advantage, garnering over 800,000 views on his campaign launch video.

He allegedly did not pay a single cent for his political campaign, although declassified documents suggest that he received a generous donation from a third party. Just one person has reportedly

donated around one million euros. Additionally, a network of accounts was used to artificially promote Georgescu's content: these accounts were created years prior to the campaign events, but they were mostly inactive until two weeks before the elections. The activity of these accounts was coordinated on external channels such as Telegram. Some of these accounts were allegedly related to Sputnik, a Russian state-owned news agency frequently described by academics and journalists as a Russian propaganda outlet, as can be found in a report compiled by the Romanian Intelligence Service. According to the report, $380,000 has been paid by an individual other than Calin Georgescu to a number of influencers who then promoted the candidate. A marketing agency was also employed. In this way, Georgescu was able to declare that he himself paid nothing for his political campaign.

While the disinformation campaign was marching on in the digital space, the IT systems put in place to monitor the voting process and aggregate the votes were also met with relentless cyberattacks. Over 85,000 different attempts to compromise the systems have been detected, including on the election day and the night after. According to the intelligence report, the way in which these attacks have been led are specific to a state actor, rather than individual activists.

Judging by the ever-increasing amount of interference attempts from the Russian state targeted towards Ukraine and its European supporters, it is safe to assume that these operations will keep going at a steady pace for the foreseeable future. As a result, the European Union must prioritize bolstering its cybersecurity defences. Physical infrastructure should be guarded at all times and systems should be kept up to date with the security updates in order to defend against new vulnerabilities. Government Officials using the IT infrastructure should always adhere to strict security protocols, like only keeping credentials in secure places. Citizens should also exercise caution in order to protect their personal data. This is especially important now, as we have moved towards an age where a significant aspect of our lives has become reliant on technology.