The Evolution of Offensive Cyberattacks and Defensive Cybersecurity Operations

2

Innovation in offensive and defensive military technologies and tactics has been a constant, especially during the past two centuries. Wars put these innovations to new tests. While the "fog of war" makes it more difficult to assess the relative strength of offensive and defensive capabilities, it also creates greater urgency for doing so. The war in Ukraine is no exception, including for cyberattacks and cybersecurity protection.

It's perhaps helpful to start with a historical analogy that is well understood. The Battle of Britain in 1940 pitted the use of an offensive technology—the bomber—against the defensive use of two other technologies, more advanced fighters, and the use of radar. The radar waves were invisible to the naked eye, and their widespread use was unknown to the public during the battle itself. But radar was indispensable in enabling the Royal Air Force to detect the oncoming bombers and direct fighters to combat them. While bombers succeeded in dropping bombs on England, they failed strategically in establishing the air supremacy needed to support an invasion.

This history shares some important similarities with the current day. The war in Ukraine has pitted offensive cyberattacks that are invisible to the naked eye against advances in cybersecurity technologies and operations. Like the bombers of 1940, some of the cyberattacks have succeeded in reaching and disabling their targets. But at a broader level, so far these attacks have failed strategically in disabling Ukraine's defenses. While part of the reason lies in the disbursement of Ukrainian digital operations into the cloud, discussed above, another reason has been the overall ability of cyber defenses to successfully defeat these attacks.

It's important to take note of the destructive cyber tactics the Russian military has deployed in Ukraine. These have three facets. The first aspect, which is also common to ransomware and nation-state cyber espionage, involves targeted phishing and similar efforts to enter a computer network. This tactic reflects the determination, sophistication, and persistence long observed across the cyber activities of Russia's intelligence community and military. The second involves the planting of "wiper" malware designed to "wipe" computer hard disks and destroy all their data. And the third has involved software architecture that is designed to replicate or spread this malware to other computers across a network domain, such as the network of an entire government ministry.