As Cyber Strikes Mount, What Happens in Ukraine Doesn't Stay in Ukraine

MARCH 30TH, 2023 BY DAVID ARIOSTO | 0 COMMENTS

CIPHER BRIEF REPORTING – The scale of Russia's cyber-attacks in Ukraine swelled in the first quarter of 2023, a top Ukrainian official told a gathering of top cyber security experts at the Cyber Initiatives Group Spring Summit on Wednesday; part of a new phase of the war to accompany an apparently stalled Russian ground campaign.

"Conventional warfare and cyber warfare are integrated things," said Col. Ivan Kalabashkin, Acting Deputy Head of the Cybersecurity Department in the Security Service of Ukraine (SSU), who detailed the nature of simultaneous Russian missile and cyber strikes against Ukrainian military positions and critical infrastructure, including recent strikes at a nuclear facility near Kyiv.

In 2022, Ukraine reported 4,500 such strikes and related incidents. That number is already at nearly 1,200 in just the first three months of 2023, Kalabashkin said. Ukraine is also dealing with around 1,000 Russian psychological and disinformation operations every month, he added.

Many of these propaganda campaigns now orient around the battle for Bakhmut, a small eastern city that has been a focal point of recent fighting. Russian forces have encircled the city but have been unable to force a Ukrainian withdraw.

Ukrainian Deputy Defense Minister Hanna Maliar addressed those operations on Wednesday, saying Russia is currently focused on three principal tasks in mass media: 1.) the undermining of civil-military trust, 2.) the discouraging of the Ukrainian army, and 3.) attempting to provoke battlefield mistakes.

"Our military command, not the Russian psychological operations, will determine how long Bakhmut will be defended," Maliar added.

And yet as the battle for Bakhmut rages, broader security questions are also being raised, not just about the evolving nature of hybrid warfare, but also about the level of public and private sector preparedness in the U.S. That preparedness includes evolving regulatory and law enforcement frameworks that govern and protect the comparably more digitally-connected societies in the West.

"What I'm really worried about is that we believe that we're safe," said General (Ret.) Keith Alexander, Cipher Brief expert and former Director of the National Security Agency, during that same Cyber Initiatives summit.

"We're not safe."

In fact, the U.S. in particular is thought to be especially vulnerable to foreign cyberattacks, according to an October report from the Foundation for Defense of Democracies, a DC-based think tank. The group identified U.S. "blind spot(s)" for cyber-focused economic warfare that could provoke "a catastrophic strategic surprise – one that could simultaneously destabilize the U.S. electrical grid, water supply, banking system, transportation sector, or other critical infrastructure necessary for survival." Hackers, for instance, who launched a cyber-attack in 2021 that disrupted fuel supplies throughout the U.S. Southeast, did so by stealing a single password. That breach occurred against a legacy virtual private network (VPN) that lacked multi-factor authentication, according to Senate testimony of Colonial Pipeline Chief Executive Joseph Blount. What that effectively means is a system that does not require a second stage in the login process, such as a text message, which is common among more modern networks.

"[Colonial Pipeline was] a wake up call," said Chris Krebs, Cyber Initiatives Group Principal and former U.S. Director of the Cybersecurity and Infrastructure Security Agency. He reflected on the attack during Wednesday's summit, which focused in part on establishing better "cyber hygiene," a reference to the maintenance and integrity of online systems. Single-factor logins are generally thought to be comparably unhygienic. Resultantly, that relatively unsophisticated attack was able to create a days-long shutdown of Colonial Pipeline, the largest fuel pipeline in the U.S., prompting widespread gas shortages and consumer panic. A subsequent report prepared by the Energy and Homeland Security Departments determined that the country could only afford at most another five days of shutdown before mass transit systems would have to begin restricting operations as a result of fuel shortages.

It is a phenomenon largely predicted by security experts, many of whom also noted that it could have been worse. In fact, it nearly was that same year when a hacker tried to poison a Florida city's water supply, increasing sodium hydroxide levels to dangerous levels. The hacker gained remote access to the Oldsmar water treatment system before luckily being thwarted by authorities before the water became toxic. Often wracked by budget cuts, as states and municipalities look to trim spending, water treatment and sewage plants are habitually considered among America's most vulnerable critical infrastructure.

Looking ahead, particularly as U.S. political season approaches, security experts are also eyeing mounting cyber threats to elections systems. Such systems are generally comprised of a variety of components, including voting machines, tabulation equipment, and official websites that can be vulnerable to hackers. Despite progress in hardening these systems, "we face continuing threats from a growing number of foreign state sponsored threat actors, intent on targeting our election infrastructure and voters through cyber activity and malign foreign influence operations," Kim Wyman, senior advisor for election security at the Cybersecurity and Infrastructure Security Agency, said on Friday.

Questions about disinformation campaigns, voter suppression, and even meddling with vote counts are coming to the forefront, she noted, alongside growing public-private sector recognition of long standing vulnerabilities in critical infrastructure.

The battlefields in Ukraine, it seems, could be just the beginning.

Read more expert-driven national security insights, perspective and analysis in The Cipher Brief

CATEGORIZED AS: CYBER | CYBER INITIATIVES GROUP | UKRAINE

TAGGED WITH: CYBER INITIATIVES GROUP | CYBERSECURITY | CYBERSECURITY SUMMIT | UKRAINE

Related Articles

CIA Director: Putin's Hold on Power Betrays "Significant Weaknesses"

CIPHER BRIEF REPORTING – A social contract that Russian President Vladimir Putin has engineered over the decades to cement his authority may now be showing signs [...] More ›

RUSSIA | UKRAINE | UNITED STATES

JULY 31ST, 2023 BY DAVID ARIOSTO

Western Focus Sharpens on China Over Black Sea Grain Deal

EXCLUSIVE SUBSCRIBER+ INTERVIEW — In the wake of a Kremlin decision to halt a U.N.-brokered Black Sea agreement, which allowed Ukraine to export tens of millions [...] More ›

CHINA | RUSSIA | UKRAINE

JULY 17TH, 2023

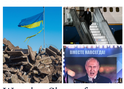
The Path to 2024's Election Is Engulfed With Novel Threats

CIPHER BRIEF REPORTING — The former head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) could scarcely be more clear in his evaluations of [...] More ›

ELECTIONS | TECH/CYBER | UNITED STATES

JULY 17TH, 2023 BY THE CIPHER BRIEF

Featured Piece



Warning Signs of a More Dangerous Global Conflict

BOTTOM LINE UP FRONT — If President Joe Biden's recent remarks in Poland and President Vladimir Putin's in Moscow just a day later are any indication of the path forward, the February 24 anniversary of the Russian invasion of Ukraine may represent the beginning of a new and potentially much more dangerous phase of the conflict, which is increasingly looking like a conflict between NATO and the Russian Federation.

FEB 22, 2023, BY ROB DANNENBERG

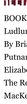
About the Cipher Brief

National security is everyone's business. The Cipher Brief is committed to publishing trusted, non-partisan information that brings together the expertise of the public and private sectors.

READ MORE

Book Reviews

View all ›



Defiance: The Latest in The Bourne Series

BOOK REVIEW: Robert Ludlum's The Bourne Defiance By Brian Freeman / G.P. Putnam's Sons Reviewed by Elizabeth C. MacKenzie Biedell The Reviewer: Elizabeth MacKenzie Biedell [...] More ›

JULY 25TH, 2023 BY THE BOURNE DEFIANCE

What the Experts Say

> The Cipher Brief's Open Source Report is an extraordinary product and an important daily read for situational awareness on national security issues.

General John R. Allen (Ret.)
Former Commander of the NATO International Security Assistance Force in Afghanistan