GEOPOLITICS

Backbone is everything, don't be owned by your infrastructure: Lessons from Ukraine for America

Russia — in its Soviet incarnation — was the source of Ukraine's infrastructure. Postwar pipes for everything from water to telecommunications in Ukraine is Russian in origin.

BY FRANK CILLUFFO AND SHARON CARDASH , FEBRUARY 28, 2022

(Getty Images)

After weeks and months of saber-rattling, Russia has brutally invaded Ukraine. Bullying autocracies are reaching back and executing old playbooks — in this instance exceptionally audaciously — and around the globe they will be looking to see how allied democracies react and respond to Russia's military aggression. For both attacker and defender, cyber domain will figure prominently. Indeed, it already has.

Consider "intelligence preparation of the battlefield," or IPB. It's what military professionals do to scope the lay of the land — both physical and virtual — before taking on their target full bore. And it's what Russia had been doing in and to Ukraine before launching fuller-scale operations.

But in the case of Ukraine, the task of IPB was immeasurably simplified for Russia. Why? Because Russia — in its Soviet incarnation — was the source of Ukraine's infrastructure. Postwar pipes for everything from water to telecommunications in Ukraine is Russian in origin.

This is a serious problem for Ukraine and its allies for a host of reasons. Among them: Communications within Ukraine and between Ukraine and its partners is effectively subject to prying Russian eyes. Absent secrecy, Ukrainian countermeasures are compromised from the get-go.

Having literally laid the groundwork in Ukraine also facilitates Russia's ability to attack regardless of Ukraine's plans to defend. Being equipped with extensive knowledge of the ins and outs of Ukraine's critical infrastructure makes it easier to undermine or take down operations.

Nor does the attacker need to engage in widespread activity in order to achieve substantial effect. Precisely because critical infrastructure sectors and functions are often interdependent, the attacker can cause outsized effect by toppling just one domino in the chain.

Cascading effects of this sort can quickly undermine the trust and confidence that a people have in their government — especially in a democracy. And trust is the coin of the realm. Without it, the bonds upon which a modern society rests can quickly fray with catastrophic results.

The lesson here is that cyber tools and tactics can be used to strategic effect as a means to an end. Moving forward, cyber domain and cyber techniques will be a fundamental dimension of warfare. In this respect, Ukraine is an object lesson for the future.

And it is one that we ignore at our peril. Now think China. Its Belt and Road Initiative (BRI) has effectively seeded large swathes of the geopolitical landscape with Chinese Communist Party infrastructure.

So what? The recipients of China's architecture are building a foundation that is composed of quicksand. While in principle advancing and modernizing through BRI, the targets of it are exposing themselves to espionage and to baked-in vulnerabilities.

Perhaps that's not a problem today or tomorrow. But the potential for future harm at a time and place of China's choosing is real. Keep in mind that compared to the West, China has shown itself to be more patient and more strategic in its thinking and in its planning.

More imminently and ominously, think Taiwan. Just as Russian President Vladimir Putin has loudly proclaimed Ukraine to be Russia's rightful backyard, so too the drumbeats from China on Taiwan are getting louder with blunt talk of reunification by Chinese officials to their Taiwanese counterparts.

It's tough to put the genie back in the bottle when it comes to all things cyber. Far better to bite the bullet at the front end and do the hard work that is necessary there. In this context, an ounce of prevention really is worth a pound of cure.

But in too many cases we must simply take the facts as we find them. Failing to take note and act accordingly will make a bad situation immeasurably worse. In the case of Taiwan — a powerhouse for semiconductor chips used heavily in the West — both U.S. national and economic security are implicated.

Put differently, if Taiwan were to fall to China, then critical U.S. infrastructure would be effectively owned by China — with our fate subject to their will. From that vantage point, America starts to look a lot like Ukraine.

China and Russia each know their cyber neighborhood intimately and are both forces to be reckoned with in this regard. But while Taiwan and Ukraine may each be outmatched by regional cyber powers who have these two countries in their target hairs, others must not be paralyzed.

Instead, America and its allies must double down on efforts to deepen resilience both within and without. There's no substitute for the ability to bounce back and thereby frustrate an aggressor. Fortunately, the best defense needn't just be a good offense.

Frank J. Cilluffo is the Director of the McCrary Institute for Cyber and Critical Infrastructure at Auburn University.

Sharon L. Cardash is the Deputy Director for Policy at Auburn University's McCrary Institute for Cyber and Critical Infrastructure.

This story was featured in CyberScoop Special Report: War in Ukraine

EXPLORE REPORT

Written by Frank Cilluffo and Sharon Cardash

In This Story

RUSSIA SUPPLY CHAIN TAIWAN UKRAINE SUPPLY CHAIN SECURITY CHINA

More Scoops

Ukraine warns of 'massive cyberattacks' coming from Russia on critical infrastructure sites

Ukrainian officials say they anticipate Russian cyberattacks in conjunction with potential missile strikes on electrical facilities

The Ukraine war could provide a cyberwarfare manual for Chinese generals eyeing Taiwan

BY TIM STARKS

Latest Podcasts

SAFE MODE — A weekly podcast on cybersecurity and digital privacy

How Troy Hunt knows if you've been hacked and Washington tries to understand AI

Why pig butchering is the worst kind of online scam

How the FBI fights ransomware

Dave Aitel on 'secure by design'; CISA's rules for cyber incident reporting

Government

FBI seeks to balance risks, rewards of artificial intelligence

CISA faces resource challenge in implementing cyber reporting rules

Space is essential for infrastructure. Why isn't it considered critical?

Ivanti-linked breach of CISA potentially affected more than 100,000 individuals

Technology

Civil society groups press platforms to step up election integrity work

Plan to resuscitate beleaguered vulnerability database draws criticism

Spyware and zero-day exploits increasingly go hand-in-hand, researchers find

Michigan lawyer in voting machine tampering case arraigned in D.C.

Threats

ALPHV steps up laundering of Change Healthcare ransom payments

Confronted with Chinese hacking threat, industrial cybersecurity pros ask: What else is new?

Intelligence officials warn pace of innovation in AI threatens US

Russian hackers accessed Microsoft source code

Geopolitics

Chinese hackers target family members to surveil hard targets

US and UK accuse China of cyber operations targeting domestic politics

German political party targeted by SVR-linked group in spearphishing campaign, Mandiant says

Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs

More Like This

Chinese hackers turn to AI to meddle in elections

BY DEREK B. JOHNSON

Cyber review board blames cascading Microsoft failures for Chinese hack

BY ELIAS GROLL

Supply chain attack sends shockwaves through open-source community

BY CHRISTIAN VASQUEZ

Top Stories

1 House hurtles toward showdown over expiring surveillance tools

BY TIM STARKS

2 FCC looks to limit how domestic violence abusers use connected cars

BY CHRISTIAN VASQUEZ

3 Extortion group threatens to sell Change Healthcare data

BY AJ VICENS