Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Emergent
Futures
Lab

Scenario One: Great Power Competition

Trends

Trend 1: *Constant contact wears thin*

The credibility of offensive cyber capabilities for deterrence derives from their use more than mere possession, driving a need to continually demonstrate capabilities at the cutting edge of an ever-changing technology stack. The highest return use has been across counter-cyber operations missions, offering options to degrade ever more aggressive and expansive hostile campaigns to buy time, as well as options for defensive responses. But the spiking ops-tempo is unrelenting…

Trend 2: *Contesting new territory, new "sovereigns," and new equities*

Some unremitting pressure on defenders and counter-cyber operators comes not merely from the adversary but from the increasing range of new players in the domain—some private sector, some otherwise neutral or even allied government entities—all pursuing their own interests and equities in the virtual battlespace through unilateral action forced by speed, complexity, and the surprising dynamics emerging from repeated competitive interactions.

Scenario Overview

Great-power competition has once more become the prevailing force shaping national security strategy, defense expenditures, and as a result, cyber operations. With their rapidly advancing capabilities, nation-states are now the primary driver of cyber conflict. Cyberspace is an increasingly anarchic field as the cool logic of mutually assured destruction has given way to a wide-open gray zone in which nation-states operate at a high tempo and constantly risk strategic miscalculation. Meanwhile, threat actors continue to proliferate in quantity and diversity, borrowing nation-state capabilities to aggressively pursue their own equities in a virtual battlespace.

Against a tense international background, covert economic activity by nation-states has turned the global free trade regime of the 1990s into a faint memory. Led by China, but joined by other states, economic espionage has escalated in scale and intensity. In Europe, states scour each other's systems for private information to bolster their own negotiating positions on trade issues. As authoritarian state firms eagerly expose Western capabilities, Western tech companies are caught in the middle, reluctant to point fingers at friendly governments but vulnerable to allegations of

complicity. In emerging markets elsewhere, rampant theft of intellectual property undercuts innovation, especially in critical sectors such as healthcare and biotech.

In the military and intelligence sphere, unexpected interaction between the many players in cyberspace makes for untimely surprises. Somewhere over Southeast Asia, a USMC F-35B witnesses a Burmese ballistic missile launch and moves to intercept—but misses, because its fused sensor suite has been compromised by another adversary. On the ground in Germany, a European Union parliamentarian leaks intelligence service documents describing POSTHARVEST, a cyber collection program that delivers implants selectively, and autonomously, to Internet of Things devices. Linked to POSTHARVEST by the leak, US-based firms are threatened with bans and fines by the parliamentarian's allies—ostensibly for human rights concerns, but in reality for protectionist reasons.

These multiplying threat actors force a new range of counter-cyber operations to develop which are increasingly cross-domain, incorporating kinetic and cyber options as well as influence, diplomacy, and grey-zone information operations. Offensive and reconnaissance capabilities are carefully calibrated to send messages not just to competitors, but also the greater threat intelligence community. DevOps software development culture further creates new opportunities for attacker advantage, accelerating the learning cycle between attacker and defender.

This new operational tempo is relentless—and it punishes no one harder than counter-operators in democratic polities. Facing a plethora of technical environments, countering operators must grapple with how to maintain capabilities across a broadening array of systems. But to minimize collateral damage, the rule of law also demands strict oversight and close familiarity with target context, driving up administrative overhead and reducing labor flexibility. Worse, these operations are increasingly conducted in a fishbowl of ever widening nonstate cyber intelligence visibility as surprising new players enter emerging market —as illustrated by the disruption of a quiet Five Eyes countering campaign intended to thwart a Daesh offshoot groups' hijacking of an NGO's disease-tracking app, which the group had sought to use to maximize contact with infectious populations in order to turn recruits into biological suicide "bombers".

Under these circumstances, democracies are on the back foot. Adversary states have become effective at exploiting the seams between the different constituent organizations of democratic societies, while bureaucratic misalignment and division hamstring these organizations' talent. And more and more, personal life is another sphere of influence to manipulate, encompassing not just frontline operators, but home, family, and friends, as IoT and wearable technologies make them part of the battlefield.

20XX Vignette #1

Captain Wiggins walked onto the ops center floor, greeted by a frantic buzz of activity as California casual analysts, uniformed officers, and tatted-up t-shirt-wearing techs clustered around workstations and digital plot tables. The threat matrix was unchanged, with no national intel inputs, but the private sector cyber intelligence feeds were flashing rapidly. Two main inbounds were highlighted on the big board, accompanied by a scatterplot sector-level victim representation and a bulleted list of salient features. As she watched, the first threat line was updated: a series of cascading failures in autonomous and electric vehicle ultra-fast charging stations using different equipment operated by multiple vendors. A previously unknown zero-day vulnerability was being exploited in a common network interface component sourced from a subcontinental third tier supplier, allowing for remote code execution of a customized payload intended to alter current restriction safety settings. Hundreds of vehicle fires were reported across dozens of EU and US cities, as green transportation initiative incentive hubs were hit in a fast-breaking campaign already claimed by anti-car activists as "revenge" for insufficiently aggressive regulatory moves to ban personal cars.

Competing for attention was a low and slow reconnaissance effort flagged in connection with identified infrastructure that was previously leveraged by Iranian Revolutionary Guards Corps' external operations cells operating in Yemen and Lebanon. Now, they were found enumerating remote turreted counter-UAV intercept systems deployed as an anti-drone defense around an ecommerce giant's warehouses. These systems were originally intended to defeat a series of harassment flights that had disrupted retail logistics for months on end during the last Christmas holiday's shopping season, but recent uncoordinated disclosure dropped after a dispute over bug bounty program payouts had demonstrated that the RF emitters could be hijacked by arbitrary third parties to target police, EMS, and other government quadcopters. The same manufacturer's systems were also deployed for protection of distributed logistics activities supporting expeditionary advance bases in multiple conflict flashpoints.

"Tell me we have something to spin up here to make this pain stop, people," said Captain Wiggins. "I'm sorry, Ma'am. The cupboard is pretty bare after last week. We just have not been able to regenerate new capability options that aren't going to be blocked nearly immediately across most backbone links by the dominant Chinese telecom providers serving the key AOs if we deploy right now…" replied her tech ops boss.

Near-Term Implications (6 months to 1 year)

- Sustained economic espionage campaigns at escalated pace, intensity, and scope
- Commercial disclosure of Western cyber operations capabilities, with influence by hostile intelligence services in both subtle and shockingly direct ways
- Hard calls around what critical infrastructure and key resource targets to defend today, and what may be acceptable losses to ensure capabilities options remain available to sustain a countering posture tomorrow

Long-Term Implications (> 5 years)

- Potentially altered relationships with historic allies and partners in cyberspace, as states face the complex geopolitical and economic realities of a changing Europe, collapsing population demographics, and the downstream impacts from budget crises
- Surprising new aggregations of talent, visibility, and risk appetites, leading to fast-moving situations in which not all players are known and not all potential moves can be accounted for, and also upending key investments in defense and intelligence functions with limited warning and long-term consequences

Scenario Author:

J.D. Work serves as the Bren Chair for Cyber Conflict and Security at the Marine Corps University (MCU), where he leads research to develop the theory, practice, and operational art of the cyber warfighting function, and to explore the wider role of the cyber instrument in national security strategy and the future defense competition and stability problem space.

Trey Herr is the Director of the Scowcroft Center for Strategy and Security's Cyber Statecraft Initiative at the Atlantic Council.

Will Loomis is a Program Assistant in the Scowcroft Center.

Twitter: @CyberStatecraft