Back in the USSA

A Game of Disruptive Operations inside the United States

ED McGrady

The national security community has recently begun focusing on the "peer" threat posed by the rather substantial militaries of Russia and China. However those competitors have learned a lot of lessons about how the United States uses military force, and how it makes national security decisions. From those lessons Russia has developed a way of challenging the US and NATO that does not necessarily involve direct military confrontation. These "gray zone" or "hybrid" operations combine all elements of conflict, from the social to political, from "kinetic" or hard power to various "non-kinetic" forms of soft power and information warfare. These forms of warfare work against free and open democracies vulnerabilities, and pose hard challenges to any defenders.

At the same time technology has increasingly enabled competent, well trained, actors to do amazing things with autonomy, information, and vehicles. Both gray zone threats and advances in civilian technology present an almost ever expanding set of threat capabilities to policy makers.

In this game we explore a technology-enabled internal and external threat to US national security. The scenario is a familiar one, Russia is in a confrontation with Poland and the Baltics. But the battlefield now expands to include the domestic for the US, with information, kinetic attacks, and other forms of hybrid warfare being exploited to disrupt, and distract, US policy makers.

The game will last 6 hours. Players will represent either US policy makers, or threat actors attempting to disrupt or distract the US in a Presidential election year. The Russian players will be working with internal US forces to distract from their ambitions in the Baltics, and from their real goal of demonstrating the ineffectiveness of NATO. The game starts a year before the election, and moves through the months prior to the election, and into the aftermath. Players will need to decide on policies, allocate resources, and work both the prevention and response problems.

The threat will not be the usual array of overly enthusiastic but under prepared group of criminals and bad actors. Instead the threat, enabled by the Russians, will have the ability to use advanced technologies in novel ways to disrupt US systems and operations. At the same time they will also be aware of any signatures they are spreading, making detection and roll up by law enforcement all the more challenging.

The game will challenge the threat players to think about the US as a system, and use their tools to disrupt that system. The US players will need to respond by creating a policy, and a response, environment where those challenges can be met.