Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Sean Wiswesser

Hybrid war is here to stay – are the Americans ready?

When a Russian missile strikes Kyiv, we recognize it as war, and one increasingly against civilians.

When a Russian agent or their intelligence services burn a warehouse in Britain, cut an undersea cable, hack a hospital network, spread disinformation online, foment racial tension, or intimidate political opponents, we call it something else. That distinction may be the West's greatest strategic mistake.

The revelations in recent weeks that Iran likely hacked water systems in the United States should come as no surprise for Americans. But it probably will.

Americans have not been prepared for the type of gray-zone warfare—attacks just below the threshold of all-out war—that Europe has been subjected to for years from Russia.

Our adversaries are experts at it, and the Iranians are raising the game in asymmetric warfare.

Both of them, and increasingly China as well, are challenging America with low-cost hacks, cyber-attacks, and, in the case of the Iranians, drone warfare that we as a country and society are not prepared for. We should expect more of the same ahead from all of these adversaries.

Threat is existential

There are key aspects of this type of warfare that Americans and all our European and NATO allies need to understand if we are to meet the challenge better.

The threat is existential to our democracies, particularly on the information-warfare and cognitive fronts. It will not get easier over time, and a whole-of-society approach is needed.

And finally, whether we believe we are at war or not, our adversaries believe in a “permanent second front” in the gray-zone. Hybrid war is here to stay and has been for a long while. We just haven’t been paying attention.

Russia and their intelligence services have been expert at the development of this new front, what they call “new generation warfare.”

> For more than a decade, Vladimir Putin's Russia has been waging a campaign against the United States and our NATO allies

For more than a decade, Vladimir Putin's Russia has been waging a campaign against the United States and our NATO allies that falls below the threshold of conventional war but achieves many of the same objectives.

It seeks to weaken our societies, undermine public confidence, divide our populations, intimidate our governments, and erode the alliances that constrain Russian power.

In my book on the same, Tradecraft, Tactics, and Dirty Tricks, I call it “Putin’s Secret War,” and the Russians have become very adept at it.

Western analysts call it hybrid warfare or gray-zone conflict, and describe it as a “new” concept that has emerged in recent years.

Russian military thinkers have been discussing it in their journals for decades, combining it with other concepts such as "non-contact warfare," and elaborating on it as a continuous struggle in which military and non-military means are fused into a single campaign.

The battlefield is not merely territory. It is information, psychology, politics, economics, and cyberspace— the targeting of our entire society.

Targeting the U.S. and Europe in war without rest

Many Western leaders still speak as though peace and war are separate conditions.

Russian strategists increasingly view them as

points on the same spectrum. In 2013, the current chief of the Russian General Staff, Valeriy Gerasimov, spoke of a “permanent second front” with “information means” that their military would increasingly depend on to counter what they saw as an assault on Russia from the color revolutions in Ukraine, Georgia and Kyrgyzstan.

But Russian hybrid warfare did not emerge overnight. It evolved from decades of Soviet and post-Soviet thinking about how a weaker power could challenge stronger adversaries without triggering a direct military confrontation.

The goal was never necessarily to defeat the NATO on the battlefield. Russian Generals are not fools. They have known since the collapse of the Soviet Union that Western airpower in particular is not a conventional threat they can match at the peer-level.

Russia’s intelligence services and military have always termed the United States the “main enemy” (glavnii protivnik).

As one Russian intelligence officer told me years ago, “All your NATO allies are second, third, etc.”

They realize they were no match for the U.S. Air Force and our allies, having witnessed the destruction of Saddam’s army from the air—twice, U.S. air campaigns in the Balkans in the 1990s and in the war-zones.

The goal then has always been to weaken the West before any battlefield ever emerged.

Russian hybrid warfare did not emerge overnight - Gen. Valeriy Gerasimov

And once at war in Ukraine, the Russians have been masters at innovation. The Ukrainians have outpaced the Russians, but Russia has far outpaced NATO in drone and electronic warfare; these are the new horizons of the next generation of war.

But at its core, hybrid war for Russia is based in the information space, and the roots stretch back to Soviet concepts of political warfare and "active measures.”

These were and remain the covert influence campaigns carried out in the shadows, designed to manipulate public opinion, exacerbate social tensions, spread disinformation, recruit agents of influence, and undermine confidence in democratic institutions.

During the Cold War, these operations involved forged documents, front organizations, propaganda campaigns and covert influence networks. Today, the same logic has been turbocharged by the internet, artificial intelligence, social media and digital communications.

But the objectives remain remarkably consistent, and not just for Russia. Iran and China also seek to find the cracks in societies

and alliances, widen them, and turn citizens and countries against one another.

Social media meddling like that conducted by the Internet Research Agency in 2016, led by Putin's former chef and oligarch Yevgeniy Prigozhin, was novel to the West at the time.

We were slow to understand then that the goal was to undermine democracy writ large, not merely influence one particular candidate or issue.

The Russians did the same in attacking the Brexit vote in the UK and every major election since, including the Hungarian election this year.

The revelation that there were more Russian spies from the SVR and GRU operating in their embassy than ever before, under a regime that seemed favorable to Russia, should remind us all as allies—Russia has no friends in the West. We are only targets.

And today cognitive AI can multiply ten-thousand-fold what was once done by human-enabled hacking and media meddling.

How to counter in the gray-zone

So what is to be done?

The first requirement is clarity. Democracies must abandon the comforting assumption that hostile activities below the threshold of conventional war are somehow less significant.

The cumulative effect of hybrid warfare can be strategically consequential even when individual incidents appear minor.

> Critical infrastructure must be hardened and not just at the federal level

The second counter lies in resilience. Critical infrastructure must be hardened and not just at the federal level.

The Iranian attacks discovered this week show all of our society needs to awaken to this challenge.

There have been other revelations in the past about deep targeting by China at every level of our government.

Cybersecurity must be strengthened, and media literacy and public awareness should be treated as components of national security rather than educational afterthoughts.

Societies that understand how influence operations work are less vulnerable to manipulation. Citizens who recognize disinformation are less likely to amplify it.

Meaningful consequences

The third requirement is deterrence. Hostile actors must believe that aggressive actions will carry meaningful consequences.

So far, for Russia and China in particular, there have been no meaningful consequences when they carry out hybrid war against the U.S. and our NATO allies.

Ambiguity is one of the principal advantages enjoyed by hybrid aggressors. The response has always been: "Well, there is no proof that they are behind it?" Really? 25-plus drone incursions into Poland in one day, crashing near military and other national security targets, and NATO could not come to a consensus?

The central challenge facing Britain, the United States, and their allies is not merely military. It is political, social, technological, and psychological

The central challenge facing Britain, the United States, and their allies is therefore not merely military. It is political, social, technological, and psychological.

The question is whether democratic societies can adapt to a world in which adversaries seek not only to defeat armies but to weaken nations from within.

History suggests they can. But history also suggests that democracies rarely respond effectively until they first acknowledge the scale of the challenge before them.

As Churchill observed in the darkest days of the twentieth century: "The great democracies still triumph, and must triumph, for they draw from every quarter the most powerful and most constant forces."

The task today is to ensure that those forces—confidence, unity, resilience, and democratic legitimacy—remain stronger than the increasingly sophisticated methods employed by those who seek to undermine them.

Churchill also famously warned in another era when democracies hesitated before a gathering threat: "The era of procrastination, of half-measures, of soothing and baffling expedients, of delays, is coming to its close."

We live in a time of consequence, and our decisions and resolve to present a more credible deterrent should reflect that.

Sean Wiswesser is a former CIA Senior Operations Officer and expert on Russian Intelligence, Espionage, and Defence Issues.