Cyber Warfare Report 1.31

Russia – Ukraine – America

Written by:

Jonathan Hollerman

Note to Reader:

Although every precaution has been taken to verify the accuracy of the information contained herein, the author and publisher assume no responsibility for any errors or omissions. No liability or responsibility is assumed for damages, losses, or injuries that may result from the use or misuse of information or ideas contained within.

To contact author or for personalized consulting go to:
www.GridDownConsulting.com

G·D·C
PREPARE FOR THE WORST

Cyber Warfare Report 1.31

There is a massive black hole in recent reporting on the escalating crisis between Russia and Ukraine, a hole so large you could drive a Mack truck through it. In typical media fashion, the politicized news coverage of the crisis in Ukraine is that something is happening "over there."

There has been little to no warning to the American people that our growing involvement in the defense of Ukraine could quickly escalate to Russian cyber-attacks on American critical infrastructure resulting in the deaths of thousands and possibly millions of Americans.

What is the current situation?

Right now, Russia has amassed 100,000 troops and massive amounts of military hardware on the border of Ukraine. Military analysts are predicting that Russia may move forward at any time in the coming days or weeks. Since Ukraine is not a member of NATO, the US is not obligated to defend that country. Regardless, it would set a bad precedent and lead to future global instability (consider the current China-Taiwan state of affairs) if the Western nations do not provide some sort of assistance to Ukraine.

The Biden administration has stated that we will not be sending our military forces into the conflict. Diplomacy with Russia has failed to avert the crisis to this point. In response, Biden and other NATO nations have warned Russia that they could experience crippling economic sanctions if they decide to invade. Up to this point, the threat of sanctions has not had the desired effect of forcing Putin to

back down from his current state of trajectory, and the Biden administration seems to be using threats of cyber-attacks against Russia as another means of deterrence.

In addition to the threat of economic sanctions, the Biden administration is foolishly telegraphing threats of cyber-attacks against the Russian mainland in response to their aggression. A couple of weeks ago, the Biden administration announced publicly that we sent US cyber warfare teams to Ukraine to assist them in the conflict. This type of "grey-zone" military activity should never be released to the public.

In response to a recent Russian cyberattack on dozens of systems within at least two Ukrainian government agencies, President Biden stated in his Jan 19 press conference,

"The question is if it's something significantly short of an... invasion or major military forces coming across… For example, it's one thing to determine that if they continue to use cyber efforts, well, we can respond the same way, with cyber."

After the press conference, White House Press Secretary Jen Psaki was asked if Russia continued to launch cyberattacks in Ukraine, would we respond in kind. She confirmed that we would do so with a "decisive, reciprocal, and united response."

What will these threats of cyber warfare lead us?

The Biden administration is threatening that if Russia uses cyber-attacks in their offensive against Ukraine, the US cyber forces may respond in kind against the Russian homeland directly. It is a pertinent question to ask if this administration understands that a cyberwar in

the electromagnetic spectrum is the future of warfare and a functional part of Russia's war doctrine as a first-strike strategy.

To most military analysts, it is a foregone conclusion that if Putin decides to advance against Ukraine, Russia will most assuredly takedown Ukraine's power grids, critical infrastructure, communication networks, and go after their government and military computer systems **before** advancing with conventional forces. That is the future of warfare: blacking out your enemy, drastically limiting their ability to wage war, and taking away the populace's access to critical infrastructures and their will to fight.

There is no credible scenario that Ukraine can win a ground war against Russia.

What they can do, however, is retaliate with cyber warfare and punish the Russians by attacking the electric grid and critical infrastructure in the Russian Homeland while trying to create societal chaos in the streets of Moscow or other large Russian cities.

A Ukrainian cyberattack against Russian infrastructure isn't mere speculation. After a recent cyber attack against the railway lines in Belarus responsible for delivering Russian military hardware to the border of Ukraine, an intelligence official in Brussels commented about Ukraine's cyber abilities,

"In Russia? What do you want turned off? How hard do you think it would be for the world's best hackers backed by a major state to wreck Russia's cyber infrastructure, black everything out, and get people killed in accidents?"

Who is the "major state" he is alluding to there? Does this intelligence official imply the US cyber warfare teams currently stationed in Ukraine?

A Ukrainian intelligence official who works in cyber activities recently stated that their country has cyber warfare capabilities to respond to a Russian invasion and that they intend to use them.

"There's always endless 'kinetic' activity between Ukraine and Russia, it's an ongoing battlefield… So, if the ground war escalates, we will escalate in cyber," he said. "But so will the Russians. But we think we can hurt them in ways they have yet to understand…"

The frightening thing with this cyberwar scenario is that Putin now knows our US cyber warfare teams are currently stationed in Ukraine and assisting them, and the Biden administration has already telegraphed that we may use cyber-attacks against Russia in response to future cyber-attacks in Ukraine.

At this point, it doesn't matter if it was a sovereign Ukrainian citizen that pushes the buttons on the keyboard to carry out cyber-attacks on the Russian Homeland or one of our US Cyberwarfare members sitting in the chair next to them… Putin will surely lay the blame for any attack on the Russian homeland at the feet of the US.

There is currently little to no discussion in the media about what a potential tit-for-tat cyberwar with Russia will look like.

If Putin believes that the US is responsible for cyber-attacks inside Russia's sovereign borders, it would be foolish to think he will not respond in kind against the US mainland. In fact, in the previous buildup of Russian forces on Ukraine's border, in April of 2021, Margarita Simonyan who is very close to Putin and considered a propaganda mouthpiece for him warned that Russia's annexing of Ukraine would lead to a "war of infrastructures" with the US including denial of internet access, shutting off power grids, and an all-out cyber offensive against US critical infrastructure.

Simonyan also suggested, "I do not believe that this will be a large-scale hot war, like World War II, and I do not believe that there will be a long Cold War. It will be a war of the third type: the cyberwar." She continued, "In conventional war, we could defeat Ukraine in two days, but it will be another kind of war. We'll do it, and then [the U.S.] will respond by turning off power to [the Russian city] Voronezh."

She goes on to postulate that Moscow would then respond with a flip of a switch, blacking out the state of Florida or New York's Harlem. **She insinuated that American military analysts and specialists are incompetent and stupid regarding this subject and that Russia would easily defeat the US in a cyberwar.**

The Biden administration is threatening to escalate a cyber-war with Russia in the electromagnetic spectrum that the US can't hope to win and a war that will dramatically affect the lives of everyday Americans inside our country. To those that don't think this is a possibility, a few days ago, in a bulletin to law enforcement and critical infrastructure entities the DHS warned,

"We assess that Russia would consider initiating a cyber-attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security," and that "Russia's threshold for conducting disruptive or destructive cyber-attacks in the Homeland probably remains very high…"

At this point, the risk of some type of US cyber-war with Russia looks to be almost inevitable if they decide to invade Ukraine.

The million-dollar question: "How far will it go, and who will back down first?"

Cyber-warfare could leave cities or states in both of our countries without access to life-sustaining infrastructures like power, sewage, and

fresh water for days or possibly weeks. But what if it doesn't stop there? A cyber war that temporarily takes critical systems off-line could quickly escalate into a cyberwar that actually "destroys" critical hardware and that could take months to replace instead of days or weeks. In a worst-case scenario, the escalation could result in Russia hitting the US homeland with a Super EMP weapon that could destroy most of the electronics in the US which would take years to repair.

What would a prolonged blackout in the US look like?

Even when the threat of cyberwar against America's Power Grid has been mentioned in the media over the last decade, very rarely is any perspective given on how a prolonged blackout would affect Americans personally. The truth is every aspect of human life in the 21st century revolves around access to electricity.

What if Putin's propagandist Simonyan, is correct and Russia does take down a state like Florida's electric power grid in response to a US cyber-attack against the Russian Homeland?

Does anyone remember the videos of chaos and death in the aftermath of Hurricane Katrina? That was an event that the government had days of warnings to prepare for, yet it still took days for FEMA to deliver basic food and water to the survivors at the Superdome. That was a localized event in New Orleans, a city of under a million people (with most having already fled the area). Now imagine an extended power blackout on the state of Florida, population 18 million, with no advanced warning, and no time for FEMA to plan how to deal with the aftermath.

The logistics of distributing food to 18 million people in Florida spread out across 66,000 square miles with no prior planning… could take weeks or months. But that's assuming that only Florida is the target.

What would our response be if Russia takes down the electric grid in one of our states or cities? Surely the Biden administration would retaliate. You can't let an attack like that go unanswered.

Where does this all go?

What if Putin takes out our entire Eastern Electric grid next. What if the cyberwar escalates and Putin takes out our national grid with an EMP which Russia's war doctrine considers part of their cyberwar arsenal? How long could the American people survive without electricity and access to basic life-sustaining needs like food, water, heat and AC, banking, no phones, TV, radio, or internet? Why are these questions not being discussed by the media today, **before** we enter a cyber conflict with another world superpower?

Most people would have no clue what is truly going on and would expect the government and military to come to their rescue at some point. **What they don't realize is that 98% of the US military is reliant on the civilian electric grid and in the same sinking boat as its citizens.** They don't know that the US government never developed a plan to deal with the aftermath of a national blackout!

Fundamentally, there is no possible way of feeding 330 million people in America without electricity, internet and communication networks, functioning food production and distribution facilities, and no interstate trucking to deliver anything. Mass starvation will ensue alongside human desperation from living in a world where survival of the fittest will become the norm.

For almost twenty years now, a little-known Congressional Committee tasked with researching the threat to the US by Electromagnetic Pulse Weapons, has been warning both Congress and the US military that a loss of the US electric grid from EMP, Cyber, solar, or a physical attack

is America's Achilles heel and a prolonged blackout from an EMP could result in the deaths of 80-90 percent of the American populace through starvation, disease, and societal collapse within the first year.

In 2019, I was a member of the joint-services Electromagnetic Defense Task Force organized by General Steven Kwast at the Lemay Wargaming Center on Maxwell AFB. We spent three days looking at the effects a national blackout would have on the US population and military. The results of the exercise and the effects a prolonged blackout would have in this country were nothing short of what I would call catastrophic. There are other individuals and national organizations that have been offering the same warnings to anyone that will listen, but the message has mostly fallen on deaf ears.

As far back as Barack Obama, administrations have been paying lip service to protecting and hardening the electric grid, yet any congressional action on the subject has either died in committee or been buried in government bureaucracy. The fact that the electric utility lobby has spent over 1 billion dollars in the last decade fighting grid hardening and federal oversight plays no small role in our current predicament.

Let's not forget about China in this discussion.

In a recent interview with NPR, China's ambassador to the United States issued the following warning "If the Taiwanese authorities, emboldened by the United States, keep going down the road for independence, it most likely will involve China and the United States, the two big countries, in a military conflict."

America doesn't have the bandwidth to enter active conflict (traditional or cyber) against two world superpowers simultaneously. If Russia does invade Ukraine, and cyber warfare around the world

escalates, it might present an opportunity for China to fast-track their plans of invading Taiwan. At a minimum, China has recently offered to provide relief to Russia to ease the effects of US and NATO financial sanctions.

In addition to the threat of cyberwar on US soil, our responses to the current situations in Ukraine and Tawain seem to be uniting and creating a bond between Russia and China. If that bond continues to grow, the geopolitical ramifications of a future Sino-Russia alliance, united against the United States, could have long-term consequences on the world stage.

Conclusion:

The sad matter of affairs is that the Biden Administration seems to be racing America headlong into a cyberwar with Russia and very few seem to understand the gravity of the situation nor the death and destruction that could take place on US soil as a result.

Our nation is on very shaky ground, and the American people are totally unaware that this little conflict on the other side of the world could have catastrophic effects on their way of life, right here **in America**.

On January 27, 1941, the Peruvian envoy to Tokyo, warned the US that their intelligence sources had learned the Japanese were about to attack Pearl Harbor. Throughout the late 1990s, FBI Agent John O'Neil was warning his superiors that Al-Qaeda terrorists were planning an attack in the US homeland.

Since 2001, Ivor van Heerden, deputy director of the LSU Hurricane Center had been sending out warnings on the inadequacy of the levees in New Orleans and the flood risk from a Hurricane. As early as 2006,

Katsuhiko Ishibashi was warning his Japanese government panel that the Fukushima Nuclear reactor, as built, was at risk of earthquakes and tsunamis.

There are hundreds of cases of early warnings not being headed throughout history resulting in mass casualties and destruction.

The difference here is that if we fail to heed the Congressional EMP Commission's warnings and a tit-for-tat US cyberwar escalates to Russia using a Super-EMP against America… we won't be counting our dead in the thousands, we will be counting our dead in the millions.

In light of this, Americans need to understand, nothing else matters. Nothing - not education policy, not race, not immigration, not taxes, not inflation, or abortion matters if no one lives. This problem is binary - either Americans demand the government make grid hardening its top priority and that we lead a global dialogue on the threats of future cyberwars, or the survival of every one of our families is placed directly in the hands of our country's worst enemies.

Jonathan Hollerman is a former military SERE (Survival, Evasion, Resistance, and Escape) Specialist, a member of the Electromagnetic Defense Task Force (EDTF), VP at EMPact America, the President of Grid Down Consulting, and a #1 bestselling author on survival and preparedness.