West Texas Cyber Security Consortium

Russia-Ukraine Crisis Could Trigger Cyber War

TEXT SIZE
Doug Bernard
April 20, 2014 6:15 AM

WASHINGTON — On the day Crimeans voted in a referendum in March on secession from Ukraine, hackers from a group calling itself the "Cyber Berkut" pelted NATO websites with online nuisance attacks designed to knock the pages offline.

While not technically sophisticated, the DDoS, or "denial of service" attacks, were enough to send several websites - including a cyber-security site in Estonia - into darkness for several hours.

NATO quickly recovered: the sites came back online, the hack attack ebbed, and no serious damage was done.

But it sent a clear message - a warning shot of sorts of things to come.

As tensions have escalated between Kyiv and Moscow, so too has the frequency of online attacks targeting a variety of government, news, and financial sites located across Ukraine and several in Russia.

So far, these attacks have amounted to mere skirmishes rather than all out cyber war.

However, with the possibility of further Russian military incursions into eastern Ukraine, a full-blown cyber war may be looming on the European continent.

And that, in turn, could draw in many more nations into the Ukrainian crisis.

Destabilizing an unstable situation

"In terms of conflict between the Western-oriented parts of Ukraine and Russia, it’s a little surprising we haven’t seen more hacking already," former Assistant Secretary of Homeland Security Stewart Baker said.

"Ukraine isn't a great power but they have some talented hackers," he said. "If there’s an area they can punch above their weight, it's cyber crime."

Baker, now a parnter at the Steptoe and Johnson law firm, said that hacking and cyber mischief are nothing new for either nation.

Ukraine is well known for harboring a large number of talented cyber criminals working for various organized crime syndicates.

"They've learned how to buy protection with the government," Baker said; "and the connections are pretty tight."

For its part, Russia has not shyed from flexing its cyber muscles, notably in Estonia in 2007 and Georgia in 2008.

Although the Kremlin never admitted responsibility, Internet analysts say that the attacks originated inside Russia and were organized by Russians.

Those attacks were likely carried out by the *Nashi*, a semi-official nationalistic Russian youth movement tied to the Kremlin, analysts say.

But Baker and other analysts note that since then Russia has invested considerable resources into building more sophisticated and potent offensive cyber capabilities, which would likely be deployed this time in a more serious cyber battle.

Complicating matters further, much of Ukraine's telecommunications infrastructure runs through lines and switches controlled by Russia.

Already this March, Ukraine's Security Service accused pro-Russian activistsin Crimea of shutting down mobile and landline phones in western Ukraine, especially targeting members of Parliament.

That combination of Russian offensive capability and access to infrastructure makes Ukraine unusually vulnerable to cyber attack. And that's a situation the Kremlin may not be able to long resist.

"You could definitely see a paired attack," Baker said, "with telecommunications shutdowns in the west crippling the government, and a more psychological warfare in the east where access to news is shut off and the zone flooded with inflammatory false reports."

"In an already unstable situation, the situation could quickly become much worse," Baker said. "This may turn out to be a new tactical strategic approach, something we haven't seen before."

Lessons from Iran

In 2012, U.S. financial institutions came under a sustained cyber attack believed to be orchestrated by Iran, but using a diffuse array of servers located around the world.

As reported by *The Washington Post*, the Obama Administration debated a forceful response to aggressively target and destroy Iranian target servers, but in the end opted for a different approach.

The administration quietly assembled a coalition of 120 nations that voluntarily agreed to choke off the Iranian attacks and they passed through their national network.

That had the effect of stopping the hack at the target end, rather than the source.

U.S. administration officials feared that an aggressive response may well have provoked a

more punishing, sustained set of attacks by Iran and its allies targeting a much larger set of American targets, analysts say.

"As good as our capabilities are, there is always the possibility for unintended consequences when you take [cyber] actions," one administration official told the Post.

That's a lesson that one leading cyber security expert seems to have taken to heart.

"Regarding the fairly muted Ukrainian response so far, Russia essentially owns Ukraine's information and communication infrastructure," said Jeffrey Carr, founder of the Internet security firm Taia Global. "It's just a matter of will for them to shut it down."

Like many security analysts, Carr believes most nation's digital infrastructures are largely unprotected from the damage a serious battle could inflict. That includes, he says, Ukraine and Russia, as well as NATO member nations and even the U.S.

That in itself, he says, may be enough to prevent a full-blown cyber war over Ukraine - but only if military tensions on the ground subside. Should Ukrainian and Russian troops come to serious blows, both sides would pull out all the stops.

"A government's going to do what a government's going to do," Carr said. "Hopefully, no one is prepared to go to war over a flimsy excuse."

Looming cyber war

The Iranian financial attacks of 2012 didn't cause much damage, and although serious, were relatively limited in scope.

But they were enough to lead some to fret about the growing possibility of serious cyber-battles that would cause long-term, possibly devastating damage.

It hasn't yet happened.

However, some analysts caution that a potentially large-scale armed conflict in Ukraine could change all that. Worse, the more serious the cyber-attack, the more hidden it may be.

"Social media, government administrations and national defense systems all rely on Internet communications," says Darren Hayes, a cyber security lecturer at Pace University.

"Cyber attacks will continue to be largely silent but potentially devastating during this conflict and could prove to be more decisive than trade sanctions or armed maneuvers," he said.

Analyst Carr sees the sorts of hacking by groups like Cyber Bekrut or Anonymous Ukraine as little more than nuisance.

"That’s an entirely lower subset of capabilities being developed by Russia in terms of attacking and shutting down infrastructure," he said.

Carr said that Russia is likely to employ a dual-pronged strategy in conflict: cutting critical services and communications in the west to isolate it from NATO and the rest of Ukraine, and blocking news in the east to flood it with bad information for a nervous populace.

And large scale cyber battles, analysts say, wouldn't be limited to the two main combatants.

Given the interconnected nature of the world today, the damage and pain could spread across Europe and around the globe.

That worries Stewart Baker, who as a former Homeland Security official, remains convinced the world - and the United States especially - is unprepared.

"I think we're really whistling past the graveyard," he said.