TIME

This KGB Chief Rang the Alarm About Russia-U.S. Cyberwars. No One Listened.

Getty Images/Cultura RF

By **SIMON SHUSTER** March 23, 2018

In the late 1980s, when he helped oversee information security at the KGB, Vladimir Rubanov already had a grasp of what cyber wars would look like in the future—and they terrified him.

The Americans had far surpassed the Russians by then in most types of technology, not least with the invention of the internet and the personal computer. At the KGB headquarters and other facilities around Moscow, Rubanov had a chance to study these machines—slow, ugly and cumbersome things by today's standards, but still advanced enough for him to realize their potential in everything his agency did best: subversion, sabotage, intelligence gathering.

“From the very beginning it was clear,” he tells TIME by phone from Moscow, where he now works mostly in the private sector. “We told our people, ‘Look, the public may not realize yet what’s going on. But we need to raise the alarm on a political level, because this stuff is a danger to our vital infrastructure.’”

The tables appear to have turned since then. The vital infrastructure now at risk is in the U.S., according to a March 15 report from the FBI and the Department of Homeland Security, which found that Russian hackers had penetrated deep into the control rooms of U.S. power stations, putting a finger on the light switch of American homes. “Since at least March 2016,” the report states, “Russian government cyber actors…targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.”

These were precisely the sorts of attacks that Rubanov had feared from the Americans. He wouldn’t comment on whether Russia was in fact responsible this time; his old habits of discretion die hard, and he still serves as an occasional adviser to the Russian government. But he did note, with a tone of regret rather than self-satisfaction, that the Americans should have listened to his warnings two decades ago.

After the KGB was dissolved in 1991 along with the rest of the Soviet Union, Rubanov went to serve on the Kremlin’s Security Council, where he was also in charge of information security. He soon got to work, along with some colleagues at the Foreign Ministry and other agencies, on drafting rules of engagement for cyber space—a “code of conduct” of the type that governs the use of nuclear and chemical weapons.

“The point was to have a kind of non-aggression pact in the cyber sphere, one that would prohibit such attacks against sovereign nations,” he says. Their hope was that these rules would eventually be adopted by the United Nations and become international law. But the effort stalled, says Rubanov, in large part because the world’s last remaining superpower wasn’t interested. “Each country wants to have guarantees of security, but it does not want to extend those guarantees to others. So this is where we ended up. In a place where no one is safe.”

Give peace a chance

Soon after Vladimir Putin took office in 2000, Russia's cyber strategy got an overhaul. The new doctrine on information security that Putin signed at the end of that year did not explicitly blame the U.S. for menacing Russia. But the implication was clear when document referred to the "desire of some countries to dominate and infringe the interest of Russia in the global information space."

A reputed technophobe, Putin had always been mistrustful of the Internet, which he has called a "CIA project." And like many of Russia's spy chiefs, he feared that microchips and operating systems imported from the U.S. were designed to function as secret tools of American sabotage, surveillance or both. But there was little he could do about it. In the field of cyber weaponry, "Russian generals felt they were losing the global arms race," Andrei Soldatov and Irina Borogan wrote in their recent book, *The Red Web*, a history of Russian cyber policy. So instead of trying to match American technology, Russia tried using diplomacy "to put some limits on the United States' offensive capabilities."

These limits would have amounted to cyber disarmament. As outlined in 2009 by one of Rubanov's successor at the Security Council, Vladislav Sherstyuk, Russia wanted a ban on cyber implants, which can act as remote-controlled bombs inside an enemy's computer networks; a ban on the use of deception to hide the source of an attack; and, a rule that would extend humanitarian law into cyber space, effectively banning attacks on civilian targets like banks, hospitals or power stations.

But the Kremlin did not have the leverage to get broad support for such a deal during the first half of Putin's tenure. In virtually all areas of digital technology, Russia still lagged far behind the U.S., and it was hopelessly dependent on foreign imports even when it came to satellite navigation for its military. Despite Putin's wish to be treated like the leader of a superpower, Russia's technological backwardness forced his diplomats to continue asking the U.S. for a peace accord in cyber space.

U.S. officials described one of these overtures in a cable dated March 2009, and despite the reserved tone of the document, it seems to suggest that the Russians were practically groveling. Andrey Krutskikh, the head of the delegation from Moscow, "gave a long monologue about how he thought the U.S. and Russia could work together in the area of cyber security," the cable states, according to a copy published the following year by Wikileaks. "He said that Russia was willing to demonstrate flexibility and 'listen to the American experience.'"

The U.S. side was unimpressed. Michele Markoff, then the acting chief of cyber affairs at the State Department, told the Russians that cyber threats could not be "usefully addressed by traditional arms control-type constraints." According to the cable, she noted that it would be "meaningless" to restrict the cyber arsenals of nation states, because they would still be able to use "proxies" to conduct their attacks in secret. The best way for Russia to deal with its concerns, Markoff suggested, would be to build up its own defenses. In other words, prepare for war.

The Wild West of cyber space

Putin has done exactly that. Over the last five years, his armed forces have raced to close the gap with the U.S. in cyber defenses. Russia's Defense Ministry and its main intelligence agency, the FSB, have both established new units devoted to this task since 2013. During a televised interview that year, Defense Minister Sergei Shoigu expressed awe at the power of what he called the new "weapons of mass destruction" in cyber space. "They can stop the water supply in major cities," he said. "They can turn off the electricity. They can block the sewer systems."

Under Shoigu, who took up his post in 2012, the Russian military has set up new "scientific squadrons" to recruit computer programmers from around the country, giving them much higher salaries and better living conditions than most other branches of the Russian armed forces. The results of such efforts have been impressive. As James Clapper, the Director of National Intelligence under the Obama Administration, told the Senate in early 2015: "The Russian cyber threat is more severe than we had previously assessed."

That was putting it mildly. By the fall of that year, the U.S. and its allies in NATO had seen a barrage of attacks attributed to Russia's new cyber forces. Among the reported targets in 2015 alone were the White House, the U.S. House of Representatives, a German steel plant, the Polish stock exchange, a French TV channel and the New York *Times*. The Russian cyber operation to sway the U.S. presidential race was up and running by the end of that year, and according to U.S. intelligence assessments, it involved hackers working both for the Russian Defense Ministry and the FSB.

As details of those intrusions have emerged over the past year and a half, some American officials and experts have come around to the idea of an international agreement on the rules of cyber war. “We went through a couple decades of essentially Wild West in this area,” Aston Carter, who served as Secretary of Defense during Obama’s second term, told a panel hosted by TIME in January at the World Economic Forum in Davos. As the discussion turned to the need for a “Digital Geneva Convention,” Carter said, “Norms and rules do matter. They define when a transgression has occurred, and they create at least potentially the possibility for collective response. I’m all for that.”

But Russia isn’t so sure anymore. As its own cyber arsenal has grown in strength, the Russian government has cooled on the idea of letting international law constrain it. One of the ironies of this apparent role reversal between the U.S. and Russia has been the position of Michele Markoff, the State Department official who essentially told the Russians to get lost when they pleaded with her for cyber disarmament in 2009.

Her more recent efforts at the U.N. have focused on much the same goal: getting international laws to apply to cyber conflict, including humanitarian laws that could ban attacks on civilian targets. But Russia has reportedly stood in her way. Last summer, when the talks on this issue broke down, Markoff wrote an impassioned complaint against the states that do as they please in cyberspace, “with no limits or constraints on their actions.” She continued: “That is a dangerous and unsupportable view, and it is one that I unequivocally reject.”

Rubanov rejects it, too. But in Moscow his voice no longer counts for much. The men who sit on the Security Council today are mostly inclined to see the tools of cyber warfare as a cheap and effective way of hurting an enemy. They are not likely to give up those tools, especially since there is no treaty prohibiting them. “If we had that document, and enough trust to verify compliance, we would be a lot better off,” says Rubanov. Now he fears it’s way too late.