The New York Times

EUROPE

German Election Mystery: Why No Russian Meddling?

By MICHAEL SCHWIRTZ SEPT. 21, 2017

BERLIN — Chancellor Angela Merkel's summons to Germany's top cabinet ministers and senior military and intelligence officials for a meeting of the Federal Security Council signaled trouble. Such gatherings are rare, typically occurring only when the country faces a grave threat like a terrorist attack.

There was just one item on the agenda that day last spring: how to protect Germany's upcoming parliamentary elections from Russian cyberattacks. At the time, it seemed almost inevitable that Germany would suffer the same fate as France and the United States, where, officials say, the Kremlin attempted to alter the results of presidential elections with "fake news" and spear phishing attacks.

But on the eve of Sunday's elections, the Russians have done something few expected: they have largely disappeared. The trolls who spread distorted and falsified information before earlier elections have failed to make much of a splash here. The websites of the campaigns and major news media outlets are operating like normal.

Germans, according to Sandro Gaycken, the director of the Digital Society Institute in Berlin, which has been monitoring for Russian meddling, are "almost disappointed that nothing is happening."

“We don’t see any verified attacks,” he said. “We’re not really expecting any Russian interference.”

In some respects, experts say, German elections are insulated from outside interference in ways those in the United States are not. The country’s politics are not as polarized as they are in the United States, where partisan enmity provided fertile ground for Russian efforts to sow confusion with distorted and falsified information amplified by Russian-controlled Twitter bots and Facebook accounts.

In a move that would seem unimaginable in the United States, the campaigns for the major political parties entered into a “gentleman’s agreement” this year not to exploit any information that might be leaked as a result of a cyberattack.

Germans also still largely trust their mainstream, traditional news media sources and, unlike Americans, tend to be wary of information disseminated on Facebook and Twitter.

Officials warn that there is still a chance that some 16 gigabytes of sensitive information stolen two years ago by Kremlin-backed hackers from Germany’s Parliament, the Bundestag, could surface, much like emails taken from the campaign of Emanuel Macron were dumped days before the election in France.

In January, someone registered two websites, btleaks.info and btleaks.org, which reminiscent of the DCLeaks website that served as a repository for documents stolen from the Democratic National Committee last year. Staffers from Germany’s domestic intelligence agency have been assigned to check those websites hourly.

But few think the information if leaked would make much difference at this point. The latest polls show Ms. Merkel in a comfortable lead ahead of her chief rivals, making it likely that she will secure a fourth term as chancellor.

So why has Russia held back?

After failing to defeat Mr. Macron or so far obtain any positive dividends from its support of the Trump campaign, it is possible, experts say, that the Kremlin has decided to rethink its approach.

Russian influence operations, or active measures as they are known, tend to work only if no one is expecting them. Unlike the Obama administration, which chose to remain silent about Russia's meddling for months before the election last November, German officials cannot seem to stop talking about the threat.

Weeks after the election of President Trump, Bruno Kahl, the head of Germany's foreign intelligence service, the BND, warned of cyberattacks aimed at "delegitimizing the democratic process" in Germany. Ms. Merkel herself has issued similar warnings.

"It makes absolutely no sense to conduct cyber-ops because everyone is waiting for it," Dr. Gaycken said. "It would almost make more sense for the C.I.A. to leak fake news to make it seem like the Russians did it."

Ripjar, a data analytics company founded by former members of Britain's Government Communications Headquarters, says that scores of automated bots on Twitter and other social media sites have been pushing anti-Merkel and anti-immigrant messaging in German. The messages appear to align with Kremlin positions ahead of the election, but do not seem to have had much resonance.

"It is a very blunt tool that I would assess has very little impact on the world," said David Balson, Ripjar's director of intelligence.

Perhaps Germany's greatest protection is not some 21st century innovation but old-fashioned paper ballots, counted by hand, that are essentially hack proof.

It would be a mistake to think the aggressive Russian interference in elections last year represented some kind of new norm, said Thomas Rid, a professor at Johns Hopkins University who is writing a book on Russian active measures. These types of operations, he said, are extremely difficult to pull off and, as the world has seen, can backfire. In many ways, he said, the Russians just got lucky.

"I think one of the risks of the 2016 operation is that we all overestimate how much you can achieve from it and how easy it is," he said. "You just can't replicate this in the country every time."

Nevertheless, Germans prepared well in advance for any hint of Russian interference.

The Federal Office for Information Security ran penetration tests looking for vulnerabilities in computer systems and software of the federal election authority. The Bundestag and the individual campaigns consulted with experts about strengthening their computer security. And major news media outlets established teams of fact checkers to protect against fake news.

German officials are now looking beyond the elections at ways to bolster the country's cyberdefenses even further.

At the Federal Security Council meeting, which was held in March, officials hammered out what has become known as the "hack-back" strategy. The plan is to try to turn the tables on the hackers, launching offensive cyberattacks against them and destroying their online infrastructure before any real damage can be done.

While the German military can now legally launch a cyber-offensive following hacker attacks on military resources, there is no provision in German law allowing for the country's cyber forces to respond to attacks on civilian infrastructure like the power grid, hospitals or servers that process election results.

"Our cyber-defenses are Swiss cheese," said Jacob Schrot, a Bundestag staffer responsible for intelligence oversight and cybersecurity matters.

Russia is not the only threat on this front. Germans are still angry about revelations made by Edward Snowden that the National Security Agency under President Barack Obama had hacked into Ms. Merkel's cellphone.

Though a precise plan of action has yet to be implemented, that federal authorities would even consider taking offensive action against an enemy is a measure of how seriously the country has come to view the cyber threat.

Enduring trauma of the Nazi era has made Germans squeamish about flexing their country's military muscles. But Russia's recent history of revanchism under President Vladimir V. Putin — not just interfering in elections but supporting hard-right nationalist parties in Europe and dabbling in military adventures, like the

annexation of Crimea and instigation of war in eastern Ukraine — has forced Germans to confront a new reality.

Marian Wendt, a member of Parliament from Ms. Merkel's party, the Christian Democratic Union, who oversees cybersecurity issues, said in an interview that Germany would prefer cooperation with Mr. Putin and Russia. But he said Germany also had a responsibility to protect itself.

"At some point you have to attack your attackers," he said.

The hack-back strategy has stirred controversy here, with some charging that it comes close to violating Germany's constitutional prohibition of offensive warfare adopted after the country's defeat in World War II. Cyber experts also question whether Germany possesses the technical expertise to pull off such a tactic, particularly against Russia's own highly advanced teams of cyber warriors.

"Our main challenge right now is a shortage of skilled I.T. security workers," said Sven Herpig, a cybersecurity expert with a German think tank, Stiftung Neue Verantwortung. "Why do we waste the few talents that we have on the offensive side when we could actually use them on the defensive side."

Germany's talk of offensive cyber actions could also escalate tensions with the Kremlin, said Mr. Rid, from Johns Hopkins University. And with Russia quiet at the moment, many question the wisdom of provoking it.

"Loose German talk of hack-back," Mr. Rid said, "could translate into Russian as 'bring it on.'"

Correction: September 22, 2017

Because of an editing error, an earlier version of this article misstated when the German elections will be held. The vote is Sunday, not Saturday.

A version of this article appears in print on September 23, 2017, on Page A6 of the New York edition with the headline: One Surprise Is Already Clear in the German Elections: No Russian Meddling.