

Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran

By David E. Sanger and Steven Erlanger

Dec. 18, 2018

WASHINGTON — *Updated Wednesday, Dec. 19: The United Nations spokesman has issued a comment about the breach and the National Security Agency said it would decline to comment. Both are included in the story below.*

Hackers infiltrated the European Union’s diplomatic communications network for years, downloading thousands of cables that reveal concerns about an unpredictable Trump administration and struggles to deal with Russia and China and the risk that Iran would revive its nuclear program.

In one cable, European diplomats described a meeting between President Trump and President Vladimir V. Putin of Russia in Helsinki, Finland, as “successful (at least for Putin).”

Another cable, written after a July 16 meeting, relayed a detailed report and analysis of a discussion between European officials and President Xi Jinping of China, who was quoted comparing Mr. Trump’s “bullying” of Beijing to a “no-rules freestyle boxing match.”

The techniques that the hackers deployed over a three-year period resembled those long used by an elite unit of China’s People’s Liberation Army. The cables were copied from the secure network and posted to an open internet site that the hackers set up in the course of their attack, according to Area 1, the firm that discovered the breach.

Area 1 made more than 1,100 of the hacked European Union cables available to The New York Times. The White House National Security Council did not have an immediate comment on Tuesday.

[Read a selection of the cables here.]

The compromised material provides insight into Europe’s struggle to understand the political turmoil engulfing three continents. It includes memorandums of conversations with leaders in Saudi Arabia, Israel and other countries that were shared across the European Union.

43. The challenge with the US Administration was that it never kept its promises. The escalation to US\$ 50 bn, then US\$ 200 bn then US\$ 500-600 bn trade affected by additional tariffs was staggering and it was unclear from where the US derived these figures. Was there really so much trade? Even US companies were shocked by this approach. The US was inconsistent, turning against the WTO and the Paris Agreement. Obama had convinced XJP to join the Paris Agreement, but now the US had withdrawn under Trump. US demands were inconsistent, illogical, and would ultimately hurt its own interests.

A portion of a cable describing a private meeting in July between European officials and Xi Jinping, the Chinese president.

But it also revealed the huge appetite by hackers to sweep up even the most obscure details of international negotiations.

The cyberintruders also infiltrated the networks of the United Nations, the A.F.L.-C.I.O., and ministries of foreign affairs and finance worldwide. The hack of the A.F.L.-C.I.O. focused on issues surrounding the negotiations over the Trans-Pacific Partnership, a trade deal that excluded Beijing.

Part of the United Nations material focuses on months in 2016, when North Korea was actively launching missiles, and appears to include references to private meetings of the world body's secretary-general and his deputies with Asian leaders.

The United Nations "has no information about "a possible cyber breach at the U.N. allegedly carried out by Chinese hackers," said a spokesman, Stephane Dujarric de la Riviere. He said cyberattacks are "only reported internally, and for most incidents the United Nations does not have sufficient information to conclusively attribute such attacks."

Some of the more than 100 organizations and institutions were targeted years ago. But many were not aware of the breach until a few days ago, when some were alerted by Area 1, a firm founded by three former officials of the National Security Agency.

The cables include extensive reports by European diplomats of Russia's moves to undermine Ukraine, including a warning on Feb. 8 that Crimea, which Moscow annexed four years ago, had been turned into a "hot zone where nuclear warheads might have already been deployed." American officials say they have not seen evidence of nuclear warheads in Crimea.

The European diplomats' account of their private meeting in July with Mr. Xi quoted the Chinese president vowing that his country "would not submit to bullying" from the United States, "even if a trade war hurt everybody."

"China was not a backward country anymore," the European note taker described Mr. Xi as saying.

In their conversations with American officials after the Helsinki meeting in July, European diplomats described efforts by the White House to engage in damage control after Mr. Trump had gone off-script during a joint news conference with Mr. Putin.



One cable quoted Mr. Xi comparing President Trump's bullying of Beijing to a "no-rules freestyle boxing match." Pool photo by Fred Dufour

Mr. Trump appeared to agree to allow Russians to question former American diplomats in exchange for the American interrogation of Russians who had been indicted by Robert S. Mueller III, the special counsel. According to a July 20 document describing their private exchanges, White House officials assured the Europeans that Mr. Trump's agreement would be "nipped down" to prevent the questioning of Americans.

A March 7 cable summarized the difficulties in relations between the United States and the European Union that had developed during the Trump administration. In it, a senior European official in Washington spoke of "messaging efforts" to deal "with the negative attitude to the E.U. in the beginning, which had created a lot of insecurity."

The official, Caroline Vicini, deputy head of the European Union mission in Washington, recommended that diplomats from the 28 member nations describe the United States as "our most important partner" even as it stood up to Mr. Trump "in areas where we disagreed with the U.S. (e.g., on climate, trade, Iran nuclear deal)."

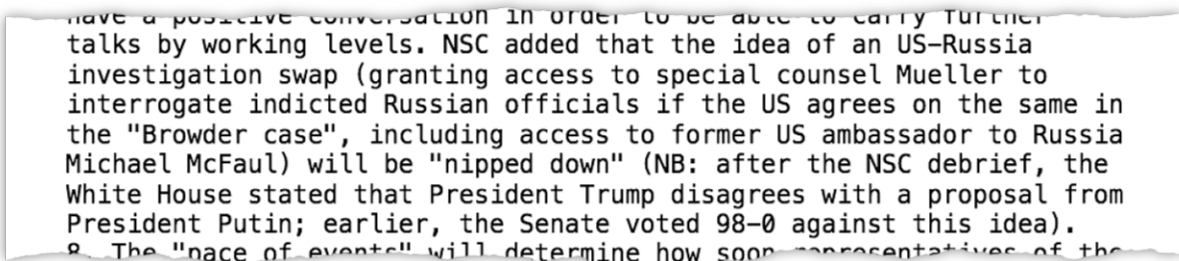
The cable also recommended working around Mr. Trump by dealing directly with Congress, and urged European diplomats in Washington to emphasize member state interest when pushing on a host of issues, including trade, renewable energy and Brexit.

In a statement on Tuesday night, the European Union's secretariat said it "is aware of allegations regarding a potential leak of sensitive information and is actively investigating the issue."

But it seemed to avoid the issues raised by the disclosure, saying it “does not comment on allegations nor on matters relating to operational security.”

The trove of European cables is reminiscent of the WikiLeaks publication of 250,000 State Department cables in 2010. But they are not as extensive and consist of low-level classified documents that were labeled limited and restricted.

The more secretive communications — including a level known as “tres secret” — were kept on a separate system that is being upgraded and replaced, according to European officials. And cables that focused on decisions about world powers’ 2015 nuclear deal with Iran — from which Mr. Trump withdrew the United States in May — are walled off from the internet in an entirely different system.



have a positive conversation in order to be able to carry further talks by working levels. NSC added that the idea of an US-Russia investigation swap (granting access to special counsel Mueller to interrogate indicted Russian officials if the US agrees on the same in the "Browder case", including access to former US ambassador to Russia Michael McFaul) will be "nipped down" (NB: after the NSC debrief, the White House stated that President Trump disagrees with a proposal from President Putin; earlier, the Senate voted 98-0 against this idea).
8. The "pace of events" will determine how soon representatives of the

A portion of a cable describing how White House officials tried to back away from statements President Trump made in a news conference with the Russian president, Vladimir V. Putin, in Helsinki in July.

Unlike WikiLeaks in 2010 or the Russian hack of the Democratic National Committee and other Democratic Party leaders in 2016, the cyberattack on the European Union made no effort to publish the stolen material. Instead, it was a matter of pure espionage, said one former senior intelligence official familiar with the issue who spoke on the condition of anonymity.

It also displayed the remarkably poor protection of routine exchanges among European Union officials after years of embarrassing government leaks around the world.

In this case, the cables were exposed after a run-of-the-mill phishing campaign aimed at diplomats in Cyprus pierced the island nation’s systems, said Oren Falkowitz, the chief executive of Area 1.

“People talk about sophisticated hackers, but there was nothing really sophisticated about this,” Mr. Falkowitz said. After getting into the Cyprus system, the hackers had access to passwords that were needed to connect to the European Union’s entire database of exchanges.

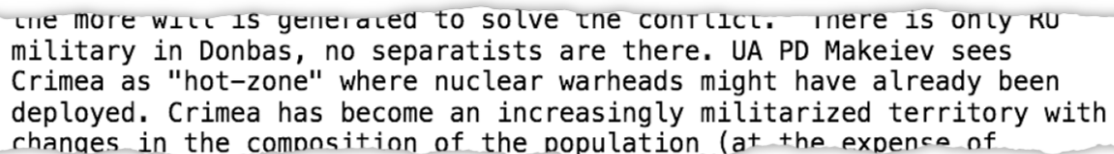
Area 1’s investigators said they believed the hackers worked for the Strategic Support Force of the People’s Liberation Army, part of an organization that emerged from the Chinese signals intelligence agency that was once called 3PLA.

“After over a decade of experience countering Chinese cyberoperations and extensive technical analysis, there is no doubt this campaign is connected to the Chinese government,” said Blake Darche, one of the Area 1’s experts.

The Chinese Embassy in Washington did not return calls for comment on Tuesday.

After burrowing into the European network, called COREU (or Courtesy), the hackers had the run of communications linking the European Union’s 28 countries, on topics ranging from trade and tariffs to terrorism to summaries of summit meetings, from the vital to the insignificant.

Many of the reports were the ordinary business of diplomacy — weekly reports from missions from places like Kosovo, Serbia, Albania, Russia, China, Ukraine and Washington, and included descriptions of conversations with leaders and other diplomats or visits to non-European countries.



the more will be generated to solve the conflict. There is only RU military in Donbas, no separatists are there. UA PD Makeiev sees Crimea as "hot-zone" where nuclear warheads might have already been deployed. Crimea has become an increasingly militarized territory with changes in the composition of the population (at the expense of

A portion of a cable describing Ukrainian concerns that Russia may have put nuclear weapons in Crimea, territory it annexed four years ago.

Among the cables were requests for authorization to finance exports to Iran, as well as details of efforts throughout 2018 to continue economic arrangements that might entice Tehran to comply with the terms of the 2015 nuclear agreement’s terms, even after Mr. Trump abandoned it.

There was also an inquiry about whether to allow Dmitry O. Rogozin, a former Russian deputy foreign minister who had called for the annexation of Crimea, to travel to Austria for an international meeting on “the peaceful uses of outer space.” At the time, Mr. Rogozin was under European financial sanctions.

There was much analysis in the cables of foreign policy and of Europe’s strategies on issues of trade, counterterrorism, migration and enlargement that could be picked apart by China and other countries looking for an advantage.

Asked about the hack, the National Security Agency said on Wednesday it would decline to comment. But the former senior intelligence official said that the European Union had been warned, repeatedly, that its aging communications system was highly vulnerable to hacking by China, Russia, Iran and other states.

The official said the warnings were usually received with a shrug.

European officials said they are now trying to overhaul their outdated and vulnerable networks — an expensive process in which technological improvements usually cannot protect against flawed human judgment. They insisted that confidential, secret and “tres secret” material is handled differently than the cables seized by the hackers and noted that a new system, known as EC3IS, is being developed to handle the more sensitive documents that are shared among the diplomats.

For communications in capitals like Moscow and Beijing, yet another network, known as Zeus, is being installed for delegations of member states.

The Europeans appear, belatedly, to be waking up to the threat. Its senior staff members increasingly use encrypted telephones, and isolated “speech rooms” of Lucite are being installed in key posts. One such room is already used for a daily 8:30 a.m. meeting of senior staff members, and another is in use in the European Council building in Brussels for intelligence briefings.

“Of course no security system is foolproof, and they must constantly be upgraded,” one senior E.U. official said.

David E. Sanger reported from Washington, and Steven Erlanger from Brussels.

A version of this article appears in print on Dec. 19, 2018, on Page A1 of the New York edition with the headline: In Hacked Cables, E.U. Frets Over Russia, China and Trump

[READ 199 COMMENTS](#)