The New York Times | https://nyti.ms/2azsuxT

EUROPE

D.N.C. Hack Raises a Frightening Question: What's Next?

The Interpreter

By AMANDA TAUB JULY 29, 2016

If Russia was indeed behind last week's leak of stolen data from the Democratic National Committee, we may be seeing one of the most sordid tools of its domestic politics deployed as a hostile weapon in foreign policy.

There is a Russian word for this practice: "kompromat." A portmanteau of the Russian words for "compromising" and "material," it refers to the timeworn tradition of obtaining information and using it to smear or influence public officials. Unscrupulous Russian politicians have been doing it for decades; there are kompromat websites (which, unsurprisingly, are often blocked or harassed).

The way it works is simple. First, Kremlin insiders or other powerful individuals buy, steal or manufacture incriminating information about an opponent, an enemy, or any other person who poses a threat to powerful interests. Then, they publish it, destroying the target's reputation in order to settle public scores or manipulate public events.

If American officials and analysts are correct in their assessment that Russia was behind this spring's hack of the Democratic National Committee's computer servers, it seems that kompromat is being translated to the international stage.

The United States has had plenty of experience with hackers, government and otherwise, but the D.N.C. hack is something new. Rather than using the information seized for intelligence purposes, the hackers selected damaging excerpts from the cache of stolen data, and then leaked them at a pivotal moment in the presidential election.

And analysts are worried that such activity could soon become a routine element of geopolitics.

"This is not just about the United States, it is not just about Trump or Clinton, or just about American democracy," said Thomas Rid, a professor of security studies at King's College London. "If they consider this a success, they may conclude that, 'Of course, we can do this elsewhere. We can do this again. We can probably also find things, kompromat, on the next president.' "

Risks with leaks

The history of kompromat in Russia shows how damaging this practice can be to democracy and the rule of law.

A 2008 article in Wired, for instance, detailed how the Kremlin leaked footage of a well-known broadcaster at an orgy to a website, apparently in order to relieve the Russian government of a prominent news media critic. In another case, leaked surveillance video showed a prosecutor investigating high-level official corruption frolicking in bed with two young prostitutes. (The investigation eventually died.)

The term may be Russian, but kompromat is not limited to the country's borders. Chinese officials and businessmen, for instance, have long been rumored to spy on their personal and professional rivals, searching for information that could be used to discredit them.

For instance, Bo Xilai, a senior party official who was jailed for corruption in 2013, reportedly wiretapped a call by China's president at the time, Hu Jintao, as part of a widespread surveillance operation that gathered information on party leaders and other powerful individuals, to aid in Mr. Bo's political ambitions.

Last week's leak of data stolen from the Democratic National Committee fits that pattern, only now it is playing out in a new arena — in an attack by one state against the political system of another.

A future of hacking

To be sure, history offers numerous examples of countries, including the United States, meddling in one another's elections. But although the aims may not be new, these technological methods and their potential consequences are.

The D.N.C. leak shows that kompromat need not reveal anything illegal to be damaging: The party's chairwoman, Representative Debbie Wasserman Schultz, had to step down after party officials were shown to have taken sides during the primaries. This sets a precedent in which virtually anyone who uses email or social media could be vulnerable to any state or private group with a grudge and access to hackers.

The Chinese and Russians are used to these tactics to settle political and business rivalries. The D.N.C. hack, in exporting kompromat abroad, has established a precedent that may tempt other hackers foreign and domestic, state-sponsored and private.

Because technology makes hacks easier to start than to counter, the risk is difficult to overcome. And anyone with money or expertise can undertake a hack, particularly against nonstate targets that have weaker security systems, and often with little risk of being caught because the attack can be denied.

"In counterintelligence before, there was a kind of granularity of targeting individuals," said Adam Segal, who studies cybersecurity at the Council on Foreign Relations and is the author of "The Hacked World Order." "And now with digital technology, you can do that with a scope and scale you couldn't have done before."

In the past, he pointed out, someone who wanted to obtain lurid details of an adversary's sex life would have had to set up a "honey trap" operation and then photograph the target in flagrante. "But now if you break into someone's email," Mr. Segal noted, "you can find a message that 'so-and-so is an idiot,' or their porn history" — private, personal information that could be tremendously embarrassing or discrediting if released.

In that climate, everyone who has something to lose, has enemies, or is a public figure is susceptible to this kind of reputational destruction. The higher a person climbs, the greater the risk becomes — and the greater temptation to a rival.

How to respond

More attacks may already be on the way. Last year, the federal Office of Personnel Management announced that hackers had breached its computers and stolen vast quantities of data gathered for security clearances and background checks.

Mr. Segal said that the stolen data included information on government employees' sex lives, relationships, finances, contacts with foreign governments and other private details.

The data, which goes back to 1985, was gathered so that American counterintelligence officers could assess employees' vulnerability to blackmail. But that well-intentioned project may have ended up conveniently cataloging their most vulnerable points for the hackers.

And on Friday, federal law enforcement officials revealed that computer systems used by the Clinton campaign had also been hacked in an attack that appeared to have come from Russia's intelligence services.

Government offices and political organizations are hardly the only targets.

In 2014, North Korea hacked Sony Pictures in retaliation for its release of the film "The Interview," a comedy about a plot to assassinate North Korea's leader, Kim Jong-un. The released emails included information on salaries, Amazon receipts for

a network executive's personal-grooming products, and plenty of embarrassing and offensive conversations. It damaged reputations and careers.

Analysts said hacking is likely to expand in the realm of foreign policy by giving states a new, low-risk method to tweak one another or to meddle in one another's internal affairs. State-sponsored hacks meant to weaponize information are relatively inexpensive and difficult to defend against, making them a tempting tool.

But it is precisely their appeal that gives these tactics the potential to make the international arena more volatile. It is hard to determine responsibility, which creates a risk that states will punish the wrong culprit — or respond too harshly, forcing an unintended cycle of escalation.

Because there are no established norms for what is and is not tolerated in such attacks, or for how a targeted state is expected to respond, even the prospect of this kind of hacking creates dangerous uncertainty.

This practice is beyond the reach or enforcement of most laws, and outside the scope of the norms that limit states' interference in one another's affairs. And because effective defense is so difficult, it is hard to predict what the limits — or the consequences — of that might be.

Follow Amanda Taub on Twitter @amandataub.

A version of this article appears in print on July 30, 2016, on Page A7 of the New York edition with the headline: Hacking of Democrats' Emails Raises Worrisome Question of What's Next.
