FUTURE
for Advanced Research & Studies

Artical Name : Hacking Democracy

Artical Subject : The Multiple Types of Electronic Breach of States' Domestic Policies

Publish Date: 20/03/2017

Auther Name: Amr Salah

Subject :

The term 'hacking' is associated by some with the traditional perception of electronic hacking exercised by technology enthusiasts. It is perceived to be one of the elements of the fifth-generation of warfare (5GW) with the aim of gathering intelligence, disabling electronics or destroying servers that are vital to the digital infrastructure of military, financial and technology institutions, thus enabling hackers to inflict losses on their enemy. However, in recent years, it turned out that hacks - in particular the cyber-attacks that states such as Russia are accused of conducting against liberal democratic regimes in the West - have evolved into wider and more diversified patterns aimed at influencing elections and domestic policies of rival governments, and even influencing the domestic balance of power in other countries.This enables states, that sponsor hacks, to achieve their interests by weakening adversaries or providing policies or electoral support to drive the rise of a favorable elements within the political circles, that could be under their control. This element party would share the same political agenda, whether publicly or privately, or embrace policies that directly or indirectly serve the interests of the states sponsoring these hacks. Types of Hacking:The following are the most common types of hacking aimed at influencing states' domestic policies. 1. Leaks: The main aim of involved states or parties ordering or directing such data breaches is to access information to leak them. Often associated with momentum, leaks aim to tarnish the reputation of certain figures and political institutions through draining their power and time by putting them on the defensive. They further intend to distract them in marginal political battles, so as to exact the highest possible moral losses on them. This is especially so when leaks are used as a pre-emptive strike in political battles that can shape the political future and electoral chances of politicians and institutions in the short or medium term. The leaks damage their chances in participating in those political battles or may even lead to their defeat.The case of failed 2016 Democratic Party presidential nominee Hillary Clinton is a good instance of how influential such electronic breaches can be. Emails sent to and from Clinton's private email server were hacked and leaked by the anti-secrecy website WikiLeaks. Russia was accused of leading the hack, which, most significantly, has extremely affected Clinton’s popularity against the then Republican nominee, Donald Trump. Rather than being focused on stepping up her campaign against her Republican rival and promoting her political agenda to the public, the Democratic nominee was distracted with defending herself and countering accusations concerning her email leaks.Political parties and figures in the 2017 elections in both Germany and France could possibly suffer from a similar campaign. This has been a growing concern of Hans-Georg Maassen, the President of the Federal Office for the Protection of the Constitution (BfV, Germany's domestic intelligence agency) who affirmed that “increasingly aggressive cyberespionage” has been occurring in the political sphere, according to a report by Deutsche Welle on December 8, 2016.Information gathered in such attacks could later be used during the election campaign “to discredit politicians”, Maassen said. He further stressed that administration officials, members of parliament and political party employees are all at risk of becoming targets.2. Hacking in support of allies: Some states or parties conduct cyber-attacks to access data and disclose such data to existing or potential allies, or those who embrace an agenda that is close to them. Such hacks further serve their allies’ interests through strengthening the status, popularity or electoral chances of certain politicians.This is evident in the press briefing that White House Press Secretary, Josh Earnest, conducted on December 16, 2016 stating that reports by US intelligence agencies confirmed that Russia had a direct role in the hacking of the servers of the Democratic National Committee (DNC). They were able to leak thousands of the Democratic Party's emails that flowed through them as well as correspondence with Clinton's campaign manager during the standoff with Republican nominee Donald Trump, who called for working with Russia. Trump publicly called for finding Clinton's missing emails, stating on July 27, 2016, "Russia if you are listening, I hope you’ll be able to find the 30,000 emails that are missing," according to a report by the New York Times.3. Hacking to blackmail and gain control: There have been cases of cyber-attacks carried out by hackers that target rivals, whether individuals or institutions, and is aimed at spying on existing or potential allies to gain access to information that enable hackers to control and direct them. Hackers gain control over the victims by blackmailing them and threatening to expose their concealed data to force them into pursuing policies that serve the interests of those behind the hacks. US intelligence agencies revealed that Russian hacks has not only targeted the Democratic Party and its nominee Hillary Clinton, but the Republican National Committee (RNC) as well. However, the information gained about the potential ally of Russia have not been revealed, which raises much speculation about the identity of the target, and some even associated the alleged hack with Russia's attempt to blackmail the Republicans and put their presidential nominee, who later won the elections, under Russia's control. This scenario became even more realistic after CNN revealed on January 12, 2017, that top US intelligence chiefs presented Trump with claims of Russian efforts to compromise him. CNN reported, “Russian operatives claimed to have compromising personal and financial information about Trump.” There are also claims that the Russians possess incriminating video footage of Donald Trump. If such incriminating evidence does exist this could be a tool, in the hands of the Russians, to blackmail Trump.4. Hacking to mislead and disseminate fake news: There are cases of hacking of the internet and social media networks which are conducted by electronic legions of tens of thousands of accounts in coordination with news website and TV channels that are affiliated to certain parties. Such groups perform the hacks directly or indirectly, and work systematically

to publish information that tarnish the image of political figures or institutions. Their aim is to create the greatest possible momentum for planned news stories that target adversaries to ensure that, when they are published, they would reach the largest possible audience despite their different technological preferences.This type of hacking included three techniques. The first involves disseminating and marketing true but negative information. In the second technique, false and negative information are disseminated, while the third involves fabricating information and news by adulterating facts with a set of lies.The third technique in particular has proven to be highly effective. False information or news story can be built on a partially true piece of information to make it look solid and consistent and gain wider circulation than true information. Rumors disseminated via the Internet against Democratic nominee Hillary Clinton were fabricated using this technique. Russian news outlets such as RT (formerly Russia Today) and Sputnik were accused of fabrication when they claimed that Clinton was diagnosed with Parkinson's disease. The story was created from information taken from an email exchange between Clinton and one of her aides and were blown out of proportion. According to Google Inc., the story was reproduced and re-published thousands of times on the Internet, which made it possible to have a readership of millions. Before the referendum on Britain's exit from the European Union was held, a large amount of information published via websites and social media outlets included great exaggerations about Britain's spending in favor of the EU. In Germany, news about the alleged rape of a 13-year-old Russian-German girl by a migrant spread and circulated rapidly across the country. The news reports sparked angry demonstrations in front of Bundeskanzleramt (the Federal Chancellery.) Shortly afterwards, it was concluded that the girl had neither been abducted nor raped, but had been absent from her family's home. The fake news prompted Hans-Georg Maassen, head of the domestic BfV intelligence agency, to say that Russia was seeking to influence public opinion ahead of the elections, and warned of the implications of Russian propaganda and its influence on voters' behavior. Former German Foreign Minister, Frank-Walter Steinmeier, too warned Russia, on January 27, 2016, against using this issue for media and political purposes. 5. Hacking to manipulate electronic voting: Former CIA employee, Edward Snowden, demonstrated how easy it is to hack into an electronic voting machine still used in several states in the US. A video he tweeted in November 2016 revealed how the data produced by the machine can be manipulated through altering its software with a PC memory card that costs just $30, enabling manipulation of voting results. Some members of the liberal opposition in the United States accused Russia of hacking electronic voting machines, in Michigan, Pennsylvania, Wisconsin, prompting some to call for a manual re-count of the ballots in the three states to verify that electronic results were not manipulated.CountermeasuresCountermeasures used in the West against cyber-attacks remain controversial. While there is almost complete consensus about countering piracy with enhanced measures to protect core technological digital infrastructures in targeted states, and fend off hackers, drafting strategies that deal with cyber-attacks pre-emptively comes at a price to the freedom of information, publication and speech. These freedoms represent a set of values established by democratic regimes as a source of much of its moral legitimacy.Despite the controversy, there are two trends in countering cyber-attacks that can be identified:1. Cyber Protection and Deterrence: In the United States, France and Germany, governments recently sought to tighten control measures to counter electronic hacks targeting their digital infrastructure. The United Sates enhanced these measures by announcing deterrent steps against Russia's hacking attempts, including expelling a group of Russian diplomats in December 2016. Germany followed suit and put similar restrictive measures in place to protect its electronic infrastructure following warnings from its domestic intelligence agencies. In France, French Defence Minister Jean-Yves Le Drian, was quoted by Reuters as saying, in an interview with French weekly Le Journal du Dimanche, "France is no less vulnerable than the United States to cyber attacks from foreign countries and the French military will boost its resources to defend against them…There is a real risk of cyber-attacks on French civil infrastructure such as water, electricity, telecommunications and transport, as well as against French democracy and the media. "2. Obstructing the Flow of Misleading Information by Verification and Transparency: To counter the spread of misleading information and propaganda, institutions and companies in the United States and Germany sought to develop what it called fact-checking technology. FactCheck.org, an interactive project of the Annenberg Public Policy Center of the University of Pennsylvania, allows any member of the public to send dubious news and stories and have their credibility verified by third-parties. The public has immediate access to the results. Stories that fails to pass the fact check will be publicly flagged as "disputed" on the internet. Analysts called upon concerned governments to pass legislation and policies that ensures transparency of information, particularly with sources of funds of news websites and outlets, and to ensure a fast and transparent flow of information with controversial issues. This, they say, would ensure audience have full and fast access to facts, while preventing hackers from exploiting rumours to serve specific purposes. Conclusion: Prospects of Technological Breaches in the WestIn Europe alone, there are 45 far-right and far-left political parties and movements, according to a study released in October 2016 by European Council on Foreign Relations. Some of them are close to Russia, and have expressed agreement with at least some recent Russian positions, including opposition to the European Union and multi-lateral international organizations, or supporting Russia's positions on Ukraine and Crimea and the lifting of international sanctions against Russia. Some of these organizations are accused of receiving funds and moral support from Russia, which raises speculation that the impact of the battle of technological breaches will not be limited to major European powers. Rather, it would expand across countries in the West to influence domestic policies through elections, referendums and other political battles in which those political organizations may gain more political support from the public and voters.