ENDGAME.

Today's Statement on Russian Hacking In Context

SERIES ONE, VOLUME ONE

ANDREA LITTLE LIMBAGO

On October 7, 1996, the Pentagon publicly attributed – without repercussions – a vast digital data breach and espionage to the Russians, later dubbed Moonlight Maze. Fast forward twenty years to the date, and President Obama publicly attributed the DNC digital attacks to Russia. Attribution is important as it publicly associates malicious activity with specific actors, while often providing evidence linking the offenders to a specific attack. Until today, there had yet to be any coherent retaliatory actions for Russian data intrusions and dumps targeting our democratic institutions.

Despite all the recent high-profile breaches, this was only the fourth time in recent years that the US government publicly attributed a digital attack. The first recent case of attribution occurred in 2014, and resulted in the indictment of five PLA officers for digital espionage. In 2015, following the Sony breach, economic sanctions were issued against North Korea. Earlier this year, the US government attributed attacks targeting banks and a dam to Iran, which resulted in the indictment of seven Iranians. Given these precedents, it seemed only a matter of time before the US responded to Russian intrusions into the integrity of our elections.

Earlier today, the Statement by the President outlined an executive order containing a multi-pronged approach to the sophisticated attacks targeting a bedrock of democracy. While likely just a first step, this is long overdue, and indicative of a whole of government, strategic approach to digital attacks. Let's break down the key points of the statement, which comprise the key aspects of a declaratory policy – the offending behavior, supporting evidence, and the repercussions.

1 Identifying the Malicious Activity – Part of any declaratory policy requires clear specification of the offending behavior to justify the response, but it also aims to deter future behavior. The Statement by the President denotes Russian interference in the election process at the highest levels, including data breaches and dumps, as well

as increased harassment of US diplomats in Russia.

2 Providing Evidence – Technical details outlining Russian activities were also released in conjunction with the Statement by the President. These range from spear phishing campaigns to exploitation of injection flaws and other vulnerabilities. DHS recommends a range of defensive measures against the Russian campaigns, helping specify how US organizations and those around the world can protect against the global campaign.

3 The Repercussions

• **Sanctions** – The US already imposed financial and economic sanctions against Russia due to the invasion of Crimea, largely focusing on Vladimir Putin's inner circle and the defense, banking, and oil and gas industries. Today's sanctions augment the Crimean sanctions, and target nine entities and individuals with links to the GRU and FSB, Russia's largest intelligence agency and state security organizations.

• **Disclosing Intel Operations** – This next step appears unique when it comes to a response to malicious digital activity. The State Department will close two Russian compounds used for Russian-intelligence in Maryland and New York.

• **Eviction** – President Obama declared thirty-five Russian intelligence operatives persona non grata. Dating back to George Washington, this implies that the thirty-five operatives and their families have 72 hours to leave the United States.

Many may argue that it is too little too late, but there is significant risk of escalation that must be weighed in conjunction with any response. The cyber domain does not occur within a vacuum. A digital tit-for-tat is not the only option. Depending on the magnitude of the attack, a government can unleash the entire arsenal of statecraft, including everything from diplomatic demarches to a military response. When major power politics (including nuclear weapons) are involved, it is essential to

minimize risk escalation and explore all possible means to provide a deterrent effect without engaging in warfare.

Today's statement not only specifies the initial US response to Russian hacking, but also is an attempt at global leadership in clarifying the appropriate standards of behavior within cyberspace. The Statement by the President emphasized the point that Russian activities are, "In violation of established international norms of behavior." The US continues to seek to establish norms through international governmental organizations such as the UN and G20, as well as bilaterally such as last year's US-Sino cooperative agreement. These various forums provide an opportunity to define which targets are deemed off limits (e.g., critical infrastructure, commercial IP), while reinforcing a focus on internet freedoms.

Unfortunately, establishing these essential norms does not occur simply through agreements, which alone are not enough as they suffer from collective action problems and compliance. They require leadership and repercussions when these norms are violated. The three most recent cases of public attribution set the foundation for the kinds of behavior which are deemed in violation of international norms, while illuminating the repercussions as well. Today's statement further established this foundation by expanding upon Russian sanctions, while also including additional retaliatory consequences against intel operations and diplomats, and disclosing the technical attributes to help protect domestic entities and global allies.

While this is an essential step, the US must take stronger leadership in pushing forth these global norms, which are extremely nascent and ill-defined to date. This requires cooperation through various forum, but just as importantly involves clear specification and repercussions if those norms are violated. Absent any repercussions, nation-states and non-state actors alike will continue to escalate digital attacks unabated.

Looking ahead into 2017, democratic institutions and freedoms remain under attack. Our European allies (e.g., France, Germany, Netherlands) have elections coming up next year. Over the last month, many have already expressed concern over Russian intervention. Today's Statement by the President notes additional steps will be taken to safeguard democratic institutions. This includes additional private and public activities, as well as a report to Congress that likely will provide additional insight into Russian activity, as may a special investigation into cyber warfare that Senators McCain, Graham, Schumer and Reed have demanded. It is essential to continue to build up and, when possible, disclose the evidence to help counter the information warfare that has become embedded within the fake news cycle, which is a key component of Russian strategy. Moreover, the US must continue to seek the dual-pronged approach of establishing norms, seeking to define acceptable rules of the road while further solidifying a declaratory policy when those formal and informal norms are violated. As these events continue to unfold, check back next week for further, technical analysis of the Russian attacks. I also will present more on this and the challenges but necessity of norm development at next month's Enigma conference.

ENDGAME.