STATEMENT FOR THE RECORD

of

Sean Kanuck
Director for Future Conflict and Cyber Security
IISS-Americas

for

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight

Hearing entitled

"Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government"

25 October 2017

10:00 am

Rayburn House Office Building

Room 2318

Chairman LaHood, Ranking Member Beyer, and distinguished Members of Congress:

It is my honor and privilege to participate in the hearing entitled "Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government" before the Subcommittee on Oversight of the Committee on Science, Space, and Technology of the House of Representatives. I thank you for your invitation and sincerely hope that my contribution will assist you in your work on this critical topic.

This Statement for the Record draws upon my twenty years of experience in the field of information and communication technologies (ICT), including: as a strategic analyst with the International Institute for Strategic Studies (IISS), as a professional attorney who specializes in cyber law, and formerly, as a senior intelligence officer for the United States Government. Although my testimony today is completely unclassified and provided in my current capacity as a think tank researcher, the perspective offered herein also benefits from my background as the National Intelligence Officer for Cyber Issues from May 2011 to May 2016. Having led cyber threat analysis for the US Intelligence Community for five years, I am quite familiar with assessing the cyber risk to both federal government and critical infrastructure systems.

My testimony will focus on assessing the risk of employing foreign ICT products and services in government networks and attempt to provide a better understanding of how they can be exploited. In my view, the present issue regarding Kaspersky Lab represents only one instance of a much larger and very complicated cyber security challenge that the US government, many other governments, and private industry all face today. While I am indeed knowledgeable of Executive Order 13800 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, I will largely defer to my fellow witnesses who are in active government service to comment on the current implementation of those policy initiatives.

1. Kaspersky Lab

In order to properly assess any risk posed by Kaspersky Lab products to the federal government, one must first understand the technical nature of those products themselves. As with many other ICT vendors and service providers, Kaspersky Lab remotely administers its services on client networks. Moreover, the very nature of Kaspersky Lab's security product offering is to provide constant and complete network monitoring to prevent and/or detect cyber intrusions and the harmful effects of malicious software. Discussions regarding the potential to introduce surreptitious "back doors" into Kaspersky Lab software are largely a moot point, because a well-known – and explicitly marketed feature – of the product offering is a wide open "front door" for Kaspersky algorithms and technicians to not only view corporate network activity (including files and traffic flows) but also to issue remedial instructions to computers on the networks they protect.

An October 2014 marketing publication by Kaspersky Lab detailed the level of system monitoring that occurs:

> "Kaspersky System Watcher scans the most relevant system event data. The monitor tracks information about the creation and modification of files, the work of system services, any changes made to the system registry, system calls and data transfers over the network. System Watcher also processes information about operations with symbolic links containing references to files or directories, modifications of the master boot record where the loader for the installed operating system is stored and interception of OS boots. Moreover, it analyses the contents of the packets transmitted via TCP, the main Internet transport layer protocol, in search of any evidence of criminal activity. The data collection process is automated and does not require user interaction."[1]

There can be no doubt that Kaspersky Lab products are thorough in their network monitoring. That is exactly what its customers are knowingly and willingly paying for, and that directly contributes to the commercial success of its business.

Another important consideration is Kaspersky Lab's ability to aggregate network information from a large and geographically diverse client base. Like other cyber security firms, cloud service providers, and telecommunications companies, Kaspersky Lab has broad visibility of activity on the Internet. As a result, it is able to detect trends and anomalies that could indicate malicious software tools, cyber intrusion efforts, and even espionage operations.[2] That capability becomes equivalent to a global cyber intelligence analysis capacity and would therefore be of high interest to many nation states. In fact, numerous press articles from October 2017 state that Israeli intelligence officers penetrated Kaspersky Lab and thereby detected Russian spying efforts that also exploited the company's access and databases.[3]

The next issue that must be considered in assessing any risk of Kaspersky Lab products to federal government systems is whether willful complicity with foreign intelligence or security services is required for such threats to manifest themselves. The answer there is a resounding "no." If the media reports mentioned above are accurate, then at least two foreign governments have already penetrated and leveraged Kaspersky Lab's cyber security products and/or international ICT network access. While the company may remain adamant that such exploitation has occurred unwittingly, the question of knowing complicity may actually be a secondary counter-intelligence concern that distracts somewhat from the underlying cyber risk concern. I respect that the United States, Israel, and other governments may be highly interested in determining if Kaspersky Lab, or any of its employees, are operating in league with the Russian intelligence and security services, but that is immaterial from a basic analytic viewpoint. If Russian operatives – or Israeli operatives for that matter – have been able to exploit Kaspersky Lab, then the answer to the question about risk to federal government systems becomes tautological. Then only remaining question then is whether Kaspersky Lab is more prone or susceptible to such activity than other cyber security vendors, for it is clear that foreign intelligence services are not limited to exploiting the products of companies originating from their own countries. National laws and regulations may, however, make it much easier for them to do so.

In the case of the Russian Federation, world-class intelligence capabilities combined with legally mandated telecommunications monitoring for law enforcement and national security purposes makes the threat very real. "Russian law gives Russia's security service, the FSB, the authority to use SORM ("System for Operative Investigative Activities") to collect, analyze, and store all data that [sic] transmitted or received on Russian networks, including calls, emails, website visits and credit card transactions. SORM has been in use since 1990 and collects both metadata and content."[4] Accordingly, any Kaspersky Lab data that electronically transits ICT networks within Russian jurisdiction could, at least theoretically, be subject to Russian government surveillance.

So once again, willful complicity may not be a required element of any foreign intelligence threat related to Kaspersky Lab. If Kaspersky Lab were required by law to render its source code to Russian authorities, or if Kaspersky Lab communications from its global operations were subject to SORM monitoring at transit points in the Russian Federation, then its mere compliance would provide Russian authorities a clear intelligence advantage. In many respects, the subject matter of this Hearing is similar to previous investigations of Chinese ICT vendors conducted by the House Permanent Select Committee on Intelligence.[5] That report concluded that, although it could not prove wrongdoing, "The investigation concludes that the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests." The analysis centered mainly on the potential for intelligence access to be derived through corporate products of foreign origin, and shifted the focus to the known espionage activities and likely intent of the foreign government. Accordingly, any discussion of Kaspersky Lab must appropriately acknowledge the Russian cyber threat.

2. Russian Cyber Operations

The Director of National Intelligence's (DNI) Worldwide Threat Assessment from May 2017, leaves no doubt that Russia remains one of the most capable cyber adversaries of the United States. His testimony before the Senate Select Committee on Intelligence stated:

> "Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure. Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture. … In some cases, Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. … We assess that Russian cyber operations will continue to target the United States and its allies to gather intelligence, support Russian decision-making, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies."[6]

Russian efforts to influence the 2016 presidential election in the United States are just the latest in a long history of Russian cyber operations. The DNI 's testimony also noted that "Outside the United

States, Russian actors have conducted damaging and disruptive cyber attacks, including on critical infrastructure networks."

If one considers Russia's intentions in cyberspace and conjoins it with the kind of information and access that could be derived from exploitation of Kaspersky Lab products and services, then the risk must be considered to be substantial. Finally, in order to determine the magnitude of that risk, one would need to look well beyond the source code of those Kaspersky products themselves. A thorough review of Russian intelligence operations, telecommunications surveillance laws, and decryption capabilities would be required, as well as a proper understanding of the Internet traffic routing patterns of Kaspersky corporate communications.

The risk associated with the Russian Federation's cyber activities must be imputed to any ICT systems or vendors over which that country's authorities are able to exercise control – wittingly or unwittingly. In this case, Kaspersky Lab's assertions that it does not collaborate with any intelligence or security services are not necessarily inconsistent with the fact that its networks could be nonetheless exploited by such services. In fact, the open source reporting previously mentioned in this Statement for the Record would seem to suggest that is a very real concern. Russian cyber operations targeting United States interests would likely leverage any avenue that could provide the desired access or information.

3. Strategic Risk Management

The final topic that I would like to concentrate on is strategic risk management of cyber threats. The greatest factor in deterring or preventing foreign cyber espionage and cyber attacks is improving the resilience of the United States' own ICT networks. That holds true for both public and private sector infrastructures. As I envision it, such resilience includes both (i) better cyber defenses to prevent intrusions, as well as (ii) alternative back-up systems to provide critical services when the primary ICT networks that we rely upon are degraded. Cost-saving measures and the convergence of ICT platforms in general (at the network, protocol, and device level) have dramatically reduced the redundancy that can provide continuity of service under adverse circumstances. Many single "points" of failure (to include persons, processes, software applications, hardware platforms, logical protocols, infrastructure nodes, etc.) are being created which threaten the robustness of the information resources that underpin the governments, industry, and the global economy.

Executive Order 13800 and the NIST Cybersecurity Framework are important steps to help safeguard critical information infrastructures. Furthermore, I believe that information security practitioners must repeatedly assess their own enterprise networks and determine not only what information assets they possess, but also, what entities might seek to compromise (e.g. steal, expose, disrupt, destroy) those assets. For entities like the United States government whose networks are obvious targets of interest for foreign cyber actors, it may be appropriate to institute profound measures that reduce potential foreign access. Banning Kaspersky Lab products from

federal systems may be one such measure, just as banning Huawei from the United States' telecommunications backbone was also deemed a necessary national security precaution.

It must be noted, however, that any such decisions may produce a reciprocal backlash from foreign governments that would adversely impact the commercial opportunities of US companies. I consider that economic policy consideration to be analytically distinct from questions of systemic cyber risk, but I am well aware that it will necessarily be part of related policy discussions. ICT vendors from the United States have already been disadvantaged as a result of previous geo-political strife, and one can presume more instances in the future. Therefore, from a policy perspective, it might be preferable to regulate or legislate against the factors and/or features that give rise to any cyber risks that are deemed unacceptable. For example, instead of outlawing Kaspersky Lab products per se, one could imagine restrictions that proscribe products of any origin that transmit US government data overseas or which maintain unfettered remote access throughout entire networks. In this regard, limitations could be imposed analogous to those that have been applied to cases brought before the Committee on Foreign Investment in the United States (CFIUS).

In conclusion, I assess that the threat of foreign cyber exploitation of Kaspersky Lab products remains a sincere concern for US federal networks. That assessment, however, rests largely on the public record of third-party exploitation, Russia's known cyber practices vis-à-vis the United States, and the inherent nature of Kaspersky's technological offerings. Willful collaboration would be a further concern, but one that is not necessarily required to assess a substantial risk. Finally, I would strongly recommend an equally rigorous analysis of the security of all ICT products used in federal networks – regardless of the national origin of the vendor – for we know that intelligence operatives are criminals alike are highly opportunistic actors.

Once again, thank you for the opportunity to provide this public service.

Respectfully submitted by Sean Kanuck, Director for Future Conflict and Cyber Security, IISS-Americas.

[1] Kasperksy Lab, "Preventing emerging threats with Kaspersky System Watcher", October 2014.

[2] Kaspersky Lab, Press Release entitled "Kaspersky Lab Identifies Operation 'Red October,' and Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide", 14 January 2013; Kaspersky Lab, Press Release entitled "Equation Group: The Crown Creator of Cyber-Espionage", 16 February 2015.

[3] The New York Times, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets", 10 October 2017; The Washington Post, "Israel hacked Kaspersky, then tipped the NSA that its tools had been breached", 10 October 2017; The Guardian, "Israel hack uncovered Russian spies' use of Kaspersky in 2015, report says", 11 October 2017.

[4] Center for Strategic and International Studies, Reference Note on Russian Communications Surveillance, 18 April 2014.

[5] Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", 8 October 2012.

[6] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, 11 May 2017.