UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

25 SEP 2022

The Honorable Chuck Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Ranking Member:

I write to provide information and documents in response to your April 28, 2022, letter to the Defense Advanced Research Projects Agency (DARPA). In addressing your inquiries, the Department must remain within legal constraints to ensure the protection of classified data. Additionally, the Department of Defense is not in a position to comment on the references in the letter that pertain to the activities of the Department of Justice. Furthermore, though the Department can share documents and information obtained from individuals affiliated with the Georgia Institute of Technology, this response should not be understood as the Department validating or endorsing that information.

The researcher identified in your letter, Dr. Manos Antonakakis of Georgia Tech, provided a proposal to DARPA as part of DARPA's Enhanced Attribution (EA) program. The purpose of EA was to explore new approaches that could identify and warn against adversary cyber actions. EA aimed to make otherwise opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing high-fidelity visibility into all aspects of malicious cyber operator actions.

DARPA issued a solicitation for EA proposals on April 22, 2016 (see Broad Agency Announcement, enclosed). The program ran from November 2016 to the fall of 2021. The EA program developed techniques and tools for generating operationally and tactically relevant information about multiple concurrent, independent malicious cyber campaigns, each involving several operators, and the means to share such information with appropriate parties. The value of such a capability is critical to national security, as cyber criminals and nation-state sponsored actors continue to escalate their activities, targeting various U.S. critical infrastructure, business, and government/military assets.

A Georgia Tech team, led by Dr. Antonakakis as Principal Investigator (PI), submitted a proposal, "Rhamnousia: Attribution Actors Through Tensor Decomposition and Novel Data Acquisition." The proposal sought to tackle the problem of systematically tracking network infrastructure used by adversary nation-state actors (see Award/Contract (Nov. 16, 2016), enclosed). The fundamental problem with cyber attribution lies within two key practical challenges: 1) finding the features necessary to assemble an attribution graph (signal identification); and 2) systematically extracting these features out of large raw data (signal extraction). To combat this problem, the Georgia Tech team built the Rhamnousia Framework

using recent advances in distributed file systems. This framework has the ability to ingest, index, and rapidly expose raw security data in the form of application programming interfaces (APIs), upon which attack-attribution analytics can be implemented. Pythia, one of the analytic services Georgia Tech prototyped, automatically created large attribution graphs from initial high confidence seed indicators (such as a domain name or IP address). These graphs provide explicit and implicit links between high confidence indicators and newly discovered – previously unknown – indicators.

While DARPA has not located documents with titles that specifically match the titles of the white papers referenced in your letter, DARPA received reports from the Georgia Tech team as part of their proposal and later participation in the EA program.

The enclosed August 7, 2016, document titled "Fancy Bear / APT28 Attribution Analysis" may correspond to the "Whitepaper on DNC attack attribution" referenced in the April 28 letter. Before the start of the EA program, the Georgia Tech team conducted research on the publicly-reported July 2016 Fancy Bear/APT-28 campaign and provided the results to researchers at DARPA, likely to highlight the capabilities of their technical approach. The Georgia Tech team had submitted a proposal for work on the EA program and had been notified they had been selected to negotiate on a contract award, but the research conducted in this report was done of their own volition and was not paid for by DARPA. The document provides an analysis of the origins of the command-and-control (C2) servers, observations about the domain registrar system used by attackers, and indicators of the attack domains being resolved by other sensitive networks.

The enclosed September 3, 2017, document titled "EOP Event Analysis" may correspond to the "Analysis of attacks of EOP (Executive Office of the President networks)" document referenced in the April 28 letter. Georgia Tech submitted this analysis to DARPA as a funded contract deliverable for their work on EA. The EOP Event Analysis report included analysis of malicious cyber activity that involved the Executive Office of the President from the time period of May 11 - June 16, 2016. As part of this analysis, the Georgia Tech team observed network traffic from AS6250, "Executive Office of the President," to IPs that were believed to be controlled by malicious cyber actors (MCAs) at that time. Georgia Tech's commercial data included global DNS data which contains traffic from many autonomous system numbers (ASNs). According to the document, the network traffic observed from the EOP was a byproduct of the analysis centered around tracking a particular malicious cyber actor group. The analysis was not designed to analyze the EOP network itself. The network traffic resolved a dynamic Domain Name System (DNS) for a host operated and managed from Hong Kong. Few other networks in the U.S. resolved this domain, and the site had passive DNS connections with the BIZCN registrar, a registrar widely known to support the DNS needs of online criminals.

The enclosed document titled "Past Russian Activities & Muller's [sic] Indictment" may correspond to the "'Mueller List – list of domains and indicators related to APT-28" document referenced in the April 28 letter. The presentation provides technical findings and attribution analysis of data from the publicly available indictment issued by Special Counsel Robert

Mueller, dated July 13, 2018. Given that the data was publicly available, DARPA asked the Georgia Tech team to provide a retrospective analysis to verify and validate tools and capabilities in development on the EA program. Georgia Tech submitted this analysis to DARPA as a funded contract deliverable for their work on EA. The analysis was able to confirm Mueller's assessment of Russian attribution and discovered additional, previously unknown, domains and IPs that could be associated with the same MCA group.

Documents corresponding to the "Whitepaper for DOJ on APT-29 related hackers, crypto coin transactions, and analysis that includes Yota-related domains" were not found in DARPA's records for the EA program.

In addition to the foregoing, enclosed please find three other Award/Contract documents between DARPA and Georgia Tech where Dr. Antonakakis participated either as PI or as Key Personnel.

I hope you find this information and enclosed documents helpful. Thank you for your support to all the men and women in the Department of Defense.

Sincerely,

Heidi Shyu

Enclosure:
As stated

cc:
The Honorable Richard Durbin
Chairman