UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
	:	
v.	:	
	:	**VIOLATIONS:**
	:	
	:	**18 U.S.C. § 371**
	:	**(Conspiracy)**
	:	
MARC BAIER,	:	**22 U.S.C. § 2778**
	:	**(Arms Export Control Act)**
RYAN ADAMS, and	:	
	:	**22 C.F.R. Parts 120-130**
DANIEL GERICKE	:	**(International Traffic in Arms**
	:	**Regulations)**
Defendants.	:	
	:	**18 U.S.C. § 1030**
	:	**(Fraud and Related Activity in**
	:	**Connection with Computers)**
	:	
	:	**18 U.S.C. § 1029**
	:	**(Access Device Fraud)**
	:	

INFORMATION

The United States charges that:

COUNT ONE
CONSPIRACY TO VIOLATE THE AECA AND THE ITAR
(18 U.S.C. § 371)

At all times material to this Information:

1. Beginning in or around December 2015 and continuing through in or around November 2019, in the District of Columbia and elsewhere, defendants MARC BAIER, RYAN ADAMS, and DANIEL GERICKE, together with others known and unknown to the United States,

did knowingly and willfully combine, conspire, confederate, and agree with each other to commit offenses against the United States, that is:

(a) to furnish defense services to persons and entities in the United Arab Emirates ("U.A.E."), and,

(b) to attempt, solicit, cause, and aid, abet, counsel, demand, induce, procure, and permit:

(i) the furnishing of defense services to persons and entities in the U.A.E.;

(ii) the reexport and retransfer of defense services and technical data to persons and entities in the U.A.E.; and

(iii) information and material protected under a January 27, 2014 Technical Assistance Agreement ("TAA") issued by the United States Department of State's Directorate of Defense Trade Controls ("DDTC") to U.S. COMPANY ONE to be provided to persons who were not authorized under the TAA to receive that information and material;

all without having first obtained the required licenses and permissions from DDTC, located in the District of Columbia, in violation of 22 U.S.C. § 2778 ("AECA"), and 22 C.F.R. Parts 120-130 ("ITAR"), in violation of 18 U.S.C. § 371.

2. The conduct alleged in this Count occurred within the District of Columbia and elsewhere, and is therefore within the venue of the United States District Court for the District of Columbia pursuant to 18 U.S.C. § 3237(a).

Goals of the Conspiracy

3. The goals of the conspiracy were to have and cause U.S. persons to furnish regulated defense services to U.A.E. CO (a privately company headquartered and organized in the

U.A.E.) and U.A.E. government entities, without a license from DDTC; to acquire information and material that was protected and governed by U.S. COMPANY ONE's TAA with DDTC; to acquire sophisticated goods and services from United States companies and to create defense articles that would be used in Computer Network Exploitation ("CNE") Operations and related activities emanating from the U.A.E.; to furnish assistance to U.A.E. persons and entities in connection with defense articles so created; to make a financial profit; and to deliver sophisticated hacking technology to U.A.E. CO and the U.A.E. government, in support of CNE Operations and related activities for intelligence gathering; all while evading the export control supervision of the United States government.

Manner and Means of the Conspiracy

4. The manner and means by which defendants sought to accomplish the objects and goals of the conspiracy included the following:

A. Defendants began planning and acting outside of the United States to have U.S. persons furnish defense services (*e.g.*, CNE Operations and related activities) to U.A.E. CO and the U.A.E. government.

B. Defendants caused and attempted to cause U.S. persons to furnish defense services to non-United States entities and persons in the U.A.E. and elsewhere without obtaining valid licenses from DDTC, which is located in the District of Columbia.

C. Defendants ignored and violated conditions placed on U.S. COMPANY ONE's TAA by knowingly obtaining and causing others to illegally obtain and disclose controlled information and material without prior approval from the United States Government, where U.A.E. CO was a competitor of U.S. COMPANY ONE for the provision of cyber services to the U.A.E government.

D. Defendants used companies outside of the U.A.E. to solicit purchase orders for U.S.-origin goods from companies located in the United States on behalf of o U.A.E. CO.

E. Defendants modified computer exploits and material in the U.A.E. into advanced covert hacking systems for U.A.E. government agencies, which defendants operated from the U.A.E.

F. Defendants used illicit, fraudulent, and criminal means, including the use of advanced covert hacking systems that utilized computer exploits obtained from the United States and elsewhere, to gain unauthorized access to protected computers in the United States and elsewhere and to illicitly obtain information, material, documents, records, data and personal identifying information, including passwords, access devices, login credentials and authentication tokens, from victims from around the world.

G. Defendants fraudulently obtained, used, and possessed access devices, authentication tokens, passwords, and other means of accessing without authorization, to gain access to those protected computers located in the United States and elsewhere.

H. Defendants were paid in the U.A.E. by the U.A.E. government (through U.A.E. CO and its affiliates) for defense services rendered by U.S. persons.

I. Defendants caused international monetary instruments to be sent from outside the United States, to the United States, to pay for U.S.-origin goods that were purchased to facilitate the provision of regulated defense services in the U.A.E.

Overt Acts

5. In furtherance of this conspiracy, and to accomplish its goals and objects, at least one of the conspirators committed or caused to be committed, in the District of Columbia, and elsewhere, at least one of the following overt acts, among others:

Violations of U.S. COMPANY ONE's TAA

A. In or around October 2015, U.A.E. CO offered employment contracts to several U.S. COMPANY ONE employees, including defendants BAIER, ADAMS and GERICKE, to leave U.S. COMPANY ONE and to join U.A.E. CO. (and, among other things, to work with a group within U.A.E. CO called Cyber Intelligence-Operations ("CIO")) with significant increases in their salaries.

B. Between in or around December 2015 and in or around February 15, 2016, defendants BAIER, ADAMS, and GERICKE, who were then employed by U.A.E. CO, attempted, and did cause, U.S. COMPANY ONE's employees to provide TAA-restricted information to defendants BAIER, ADAMS, and GERICKE, in violation of the conditions and terms of U.S. COMPANY ONE's TAA, without necessary preapproval from the United States government.

Provision of Defense Services

C. Between in or around January 2016 and in or around May 2016, defendant BAIER obtained an agreement from U.S. COMPANY FOUR in the United States to provide EXPLOIT ONE (an exploit which provided "zero-click" remote access to smartphones and mobile devices using certain versions of U.S. COMPANY TWO's operating system) and other computer exploits to U.A.E. CO in exchange for

approximately $750,000, and thereafter caused U.A.E. CO to send approximately $1,300,000 via wire transfers from a company controlled by U.A.E. CO.

D. Starting in or around May 2016, using EXPLOIT ONE, defendants BAIER, ADAMS, GERICKE, designed, implemented, modified, and used a remote computer exploitation system for foreign intelligence gathering purposes, known as KARMA, that was fully integrated into CIO's computer infrastructure to further CIO's CNE Operations and related activities.

E. In or around September 2016 (after U.S. COMPANY TWO's new operating system patched the vulnerability being exploited by EXPLOIT ONE and the KARMA system), defendant BAIER contacted U.S. COMPANY FIVE, which was located in the United States, to obtain EXPLOIT TWO, another exploit that utilized a different vulnerability in the U.S. COMPANY TWO's operating system.

F. Between in or around September 2016 and in or around January 2017, defendant BAIER caused U.A.E. CO to send over $1,300,000 via wire transfers from a company controlled by U.A.E. CO to U.S. COMPANY FIVE located in the United States. These payments were for the purchase of EXPLOIT TWO and another computer exploit.

G. Between in or around September 2016 and in or around January 2019, using EXPLOIT TWO, defendants BAIER, ADAMS, and GERICKE designed, implemented, modified, and used KARMA 2, a remote computer exploitation system for foreign intelligence gathering purposes known as KARMA 2, which was fully integrated into CIO's computer infrastructure to further CIO's CNE Operations and related activities.

H. Between in or around December 2015 and in or around July 2019, defendants BAIER, ADAMS and GERICKE purchased and obtained numerous proprietary computer exploits from companies around the world to be deployed against computers (*e.g.*, smartphones) using U.S. companies' software, services, and internet browsers.

I. Between in or around October 2015 and the present day, none of the defendants applied to DDTC, located in the District of Columbia, for a license, or a TAA, to provide defense services to U.A.E. CO, the U.A.E. government, or to any other foreign person or country, despite the fact that the conduct described above in paragraphs D-H constituted a defense service for which a license was required under the ITAR and USML Category XI(b) and (d).

(**Conspiracy to Violate the AECA and the ITAR**, in violation of Title 18, United States Code, Section 371)

COUNT TWO
CONSPIRACY TO COMMIT ACCESS DEVICE FRAUD AND COMPUTER HACKING OFFENSES
(18 U.S.C. § 371)

6. Paragraphs 1 through 5 are re-alleged here.

7. Beginning in or around December 2015 and continuing through in or around November 2019, beginning outside of the jurisdiction of any particular State or district and later occurring within the District of Columbia and elsewhere, and therefore, pursuant to 18 U.S.C. §§ 3237(a) and 3238, within the venue of the United States District Court for the District of Columbia, defendants BAIER, ADAMS, and GERICKE, together with others known and unknown to the United States, did knowingly and willfully combine, conspire, confederate, and agree with each other to commit the following offenses against the United States:

(a) For purposes of private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, that is, (i) access device fraud, in violation of 18 U.S.C. §1029(a)(2), and (ii) the provision of defense services without a license, in violation of 22 U.S.C. § 2778, intentionally access, and attempt to access, computers without authorization, and thereby obtain, and attempt to obtain, information from protected computers, in violation of 18 U.S.C. §1030(a)(2) and (c)(2)(B)(i) and (ii);

(b) Knowingly cause, and attempt to cause, the transmission of a program, information, code, computer exploits, and commands, and as a result of such conduct, intentionally cause, or attempt to cause, damage without authorization to 10 or more protected computers during a one-year period, in violation of 18 U.S.C. §1030(a)(5)(A) and (c)(4)(B);

(c) Knowingly, and with intent to defraud, use one or more unauthorized access devices during any one-year period, and by such conduct obtain a thing of value in excess of $1,000, in violation of 18 U.S.C. § 1029(a)(2), and (c)(1)(A)(i); and

(d) Knowingly, and with intent to defraud, possess fifteen or more unauthorized access devices, in violation of 18 U.S.C. §1029(a)(3) and (c)(1)(A)(i).

Goals of the Conspiracy

8. The goals of the conspiracy were to obtain financial profit and personal compensation, and other private gain for defendants BAIER, ADAMS, and GERICKE; create, operate, and maintain electronic systems specially designed for CNE Operations and related activities; obtain computer infrastructure (*e.g.*, online accounts, servers, and anonymizing services) for purposes of CNE Operations and related activities; illicitly, through CNE Operations

and other means, acquire data, information, and material from persons and organizations for provision to, and use by, U.A.E. CO; to acquire sophisticated goods and services from companies inside and outside the United States in furtherance of CNE Operations and related activities; to evade and avoid detection by foreign countries, providers of compromised devices and software (including U.S. companies); to utilize computers, servers, and infrastructure around the world, including in the United States, to facilitate CNE Operations; and to hire and acquire personnel highly skilled and trained in CNE Operations and related activities.

Manners and Means of the Conspiracy

9. In addition to the manner and means alleged in Paragraph 4, the manner and means by which defendants sought to accomplish the objects of the conspiracy included the following:

A. Defendants provided CNE Operations and related activities for U.A.E. CO;

B. Defendants established, operated, maintained, and expanded CIO into a multi-faceted and a sophisticated computer hacking organization, by: (i) hiring skilled U.S. person and other non-Emirati employees with technical expertise; (ii) obtaining, developing, modifying, and using computer exploits, malware, proxy servers, and other computer hacking tools and infrastructure on behalf of CIO; and (iii) obtaining, developing, modifying, maintaining and using internet and computer infrastructure on behalf of CIO;

C. Defendants obtained, developed, modified, maintained, and used electronic systems designed for intelligence purposes, to collect information without authorization from internet-connected computers, databases, and electronic systems in the United States and elsewhere;

D. Defendants led, managed, conducted, supported, and abetted CIO's CNE Operations and related activities;

E. Defendants damaged protected computers, including protected computers located in the United States and elsewhere, without authorization through exploits and malicious agents or implants which provided unauthorized access to said computers;

F. Defendants stole and fraudulently obtained, used, and trafficked in access devices, authentication tokens, passwords, and other means of accessing without authorization protected computers, including protected computers located in the United States and elsewhere, belonging to individual account and computer owners, for the purpose of committing additional CIO CNE Operations and related activities through the fraudulent use of said access devices, authentication tokens, and passwords; and

G. Defendants obtained information of value that belonged to the owners and users of the protected computers, including protected computers located in the United States and elsewhere, such as personal and user data, communications, access devices, authentication tokens, and passwords.

Overt Acts

10. In addition to the acts alleged in Paragraph 5, which are re-alleged here, and in furtherance of the conspiracy, and to accomplish its goals and objects, at least one of the conspirators committed or caused to be committed, in the District of Columbia and elsewhere, at least one of the following overt acts, among others:

A. Between in or around January 2016 and in or around August 2019, defendants BAIER, ADAMS, and GERICKE used stolen login credentials and other authentication tokens to obtain personal and private data from protected computers, including data held on U.S. COMPANY TWO and U.S. COMPANY THREE computers in the United States.

B. Between in or around January 2016 and in or around November 2019, defendants BAIER, ADAMS, and GERICKE purchased and used anonymization services and related equipment from a company in the United States for the purpose of hiding CIO's CNE activities.

C. Between in or around January 2016 and in or around November 2019, defendants BAIER, ADAMS, and GERICKE created and used accounts from numerous U.S. companies (including U.S. COMPANY TWO and U.S. COMPANY THREE) to conduct CNE operations and transmit programs such as KARMA and KARMA 2.

(**Conspiracy to Commit Access Device Fraud and Computer Hacking Offenses**, in violation of Title 18, United States Code, Section 371)

Respectfully Submitted,

CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY
FOR THE DISTRICT OF COLUMBIA

9/14/2021
DATE

By: _____
Tejpal S. Chawla
Demian Ahn
Assistant United States Attorneys

MARK LESKO
ACTING ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

9/14/2021
DATE

By: _____
Ali Ahmad
Scott Claffee
Trial Attorneys
Counterintelligence & Export Control Section