UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	**UNDER SEAL**
	)	
v.	)	Violations: Title 18, United States Code, Sections 371, 1028A,
	)	
JIA WEI (贾 伟)	)	1030(a)(2)(C), and 1343
also known as "chansonJW," "JWT," "JWT487," "asmikace," "asmikace3d," "askikace3d," and "haber william"	)	**SUPERSEDING INDICTMENT**

22 CR 00127

Judge Shah
Magistrate Judge Cox

COUNT ONE

The SPECIAL MAY 2021 GRAND JURY charges:

1. At times material to this indictment:

a. The People's Liberation Army ("PLA") was the military of the People's Republic of China ("PRC").

b. Military Unit Code Designator 61786 ("Unit 61786") was a signals intelligence component of the PLA, and generally worked to obtain communications and information of third parties without authorization through hacking. Unit 61786 was part of the PLA's General Staff, Third Department, First Bureau, and was located in the Haidian District of Beijing, PRC.

c. JIA WEI, pictured in Exhibit A, was a member of the PLA, assigned to Unit 61786.

d. Company A was a multi-national corporation headquartered in the Northern District of Illinois. Among other products, Company A sold communication devices worldwide. Company A maintained computer servers in the Northern District of Illinois that were used to support its sales of products in

interstate and foreign commerce. Company A restricted access to its computer network to employees or other authorized users through passwords and other means.

e. Individuals J.Y. and J.N. were two individuals who were provided a login and password by Company A for legitimate access to Company A's private computer network.

f. Company B, headquartered in the PRC, was a competitor of Company A that also sold communication devices. On or about March 14, 2017, Company A sued Company B for theft of its communications device-related trade secret information.

2. From no later than March 2, 2017, and continuing through at least June 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI,
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "askikace3d," and "haber william"

defendant herein, and others unknown to the Grand Jury, devised, intended to devise, and participated in a scheme to defraud Company A and to obtain property belonging to the Company A, by means of materially false and fraudulent pretenses, representations, and promises, which scheme is further described below.

3. It was part of the scheme that defendant and co-schemers, including other members of Unit 61786, fraudulently obtained access to Company A's computer network without Company A's authorization to obtain Company A's non-public and propriety information for the benefit of PRC-based entities.

4. It was further part of the scheme that, beginning on or about March 2,

2017, and continuing through approximately June 2017, defendant and co-schemers accessed and attempted to access the computer network of Company A without authorization. For instance, defendant fraudulently obtained the Company A login and password of Individual J.Y. and Individual J.N. and used those credentials to access the Company A computer network without Company A's authorization or consent.

5. It was further part of the scheme that after obtaining unauthorized access to Company A's computer network, defendant and his co-schemers caused non-public and proprietary information, including information related to internal competitive intelligence about Company B, to be transferred from the Company A's computer network to another computer under the co-schemers' control, without Company A's authorization or consent.

6. It was further part of the scheme that, between on or about March 16, 2017, and on or about March 23, 2017, defendant and his co-schemers caused approximately 1,094 documents to be exfiltrated or transferred from Company A's computer network to a computer used or controlled by the defendant and his co-schemers. Some of these documents related to civilian and military communication devices of Company A and Company A's competitors, and included product development information, testing plans, and internal evaluations of Company A's products, and commercial information about Company A's competitors. Around the same time, defendant also copied Company A documents discussing Company B, including a competitive intelligence document about Company B that was

downloaded four times. These documents were accessed and exfiltrated from Company A's computer network approximately 35 hours after Company A filed its civil lawsuit alleging trade secret theft by Company B pertaining to some of the same communication devices' technology.

7. It was further part of the scheme that on or about April 14, 2017, during the unauthorized access to Company A's network, defendant and his co-schemers attempted to install malware, which is malicious software designed to assist with the continued unauthorized access to Company A's computer network, on Company A's computer network without Company A's knowledge, authorization, or consent.

8. It was further part of the scheme that between on or about May 17, 2017, and on or about May 25, 2017, defendant and co-schemers transferred an unknown number of additional documents from Company A without Company A's authorization or consent through encrypted file transfers to computer servers used or controlled by defendant and his co-schemers.

9. It was further part of the scheme that defendant created online accounts using alias names to conceal, misrepresent, and hide his identity.

10. It was further part of the scheme that defendant and his co-schemers concealed, misrepresented, and hid, and caused to be concealed, misrepresented and hidden, the existence, purpose and acts done in furtherance of the scheme.

11. On or about March 14, 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

defendant herein, for the purpose of executing the above-described scheme, knowingly transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, and signals from a place outside Illinois, namely, the defendant's unauthorized access via the Internet of Company A's computer network, using the login and password assigned to Individual J.Y., which computer network was located in in the Northern District of Illinois;

In violation of Title 18, United States Code, Section 1343.

COUNT TWO

The SPECIAL MAY 2021 GRAND JURY further charges:

1. Paragraphs 1 through 10 are incorporated here.

2. On or about May 24, 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

defendant herein, for the purpose of executing the above-described scheme, knowingly transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, and signals from a place outside Illinois, namely, the defendant's unauthorized access via the Internet of Company A's computer network, using login credential of Individual J.N., which computer network was located in in the Northern District of Illinois;

In violation of Title 18, United States Code, Section 1343.

COUNT THREE

The SPECIAL MAY 2021 GRAND JURY further charges:

1. Paragraphs 1(a) through 1(f) of Count One of this indictment is incorporated here.

2. From on or about March 2, 2017 through at least June 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

did conspire with individuals unknown to the grand jury, including other unknown members of Unit 61786, to intentionally access a computer used in interstate and foreign commerce without authorization and exceeded authorized access and thereby obtained information from a protected computer, namely the computer network of Company A, and (1) the offense was committed for purposes of commercial advantage; (2) the offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud; and (3) the value of the information obtained exceeds $5,000; in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i), (c)(2)(B)(ii), and (c)(2)(B)(iii).

3. It was part of the conspiracy that defendant and co-conspirators, including other members of Unit 61786, obtained access to Company A's computer network without Company A's authorization to obtain Company A's non-public and propriety information for the benefit of PRC-based entities.

4. It was further part of the conspiracy that, beginning on or about March 2, 2017, and continuing through approximately June 2017, defendant and co-conspirators accessed and attempted to access the computer network of Company A without authorization. For instance, defendant fraudulently obtained the Company A login and password of Individual J.Y. and Individual J.N. and used those credentials to access the Company A computer network without Company A's authorization or consent.

5. It was further part of the conspiracy that after obtaining unauthorized access to Company A's computer network, defendant and his co-conspirators caused non-public and proprietary information, including information related to internal competitive intelligence about Company B, to be transferred from the Company A's computer network to another computer used or controlled by defendant and his co-conspirators, without Company A's authorization or consent.

6. It was further part of the conspiracy that, between on or about March 16, 2017, and on or about March 23, 2017, defendant and his co-conspirators caused approximately 1,094 documents to be exfiltrated or transferred from Company A's computer network to a computer used or controlled by defendant and his co-conspirators. Some of these documents related to civilian and military communications devices of Company A and Company A's competitors, and included product development information, testing plans, and internal evaluations of Company A's products, and commercial information about Company A's competitors. These documents were accessed and exfiltrated from Company A's computer network

approximately 35 hours after Company A filed its civil lawsuit alleging trade secret theft by Company B pertaining to some of the same communication devices' technology.

7. It was further part of the conspiracy that on or about April 14, 2017, during the unauthorized access to Company A's network, defendant and his co-conspirators attempted to install malware, which is malicious software designed to assist with the continued unauthorized access to Company A's computer network, on Company A's computer network without Company A's knowledge, authorization, or consent.

8. It was further part of the conspiracy that between on or about May 17, 2017, and on or about May 25, 2017, defendant and co-conspirators transferred an unknown number of additional documents from Company A without Company A's authorization or consent through encrypted file transfers to computer servers used or controlled by defendant and his co-conspirators.

9. It was further part of the conspiracy that defendant created online accounts using alias names to conceal, misrepresent, and hide his identity.

10. It was further part of the conspiracy that defendant and his co-conspirators concealed, misrepresented, and hid, and caused to be concealed, misrepresented and hidden, the existence, purpose and acts done in furtherance of the conspiracy.

Overt Acts

11. In furtherance of the conspiracy and to effect its objects and purposes, defendant committed and caused to be committed the following overt acts, among others, within the Northern District of Illinois and elsewhere:

a. From approximately March 2, 2017 to approximately June 2017, defendant and his co-conspirators attempted to access Company A's computer network.

b. On or about March 14, 2017, defendant and his co-conspirators accessed Company A's computer network with the login and password assigned to Individual J.Y.

c. From on or about March 16, 2017 to March 23, 2017, defendant and his co-conspirators exfiltrated or transferred documents from Company A's computer network.

d. On or about April 17, 2017, defendant and his co-conspirators attempted to install software on Company A's computer network.

e. From on or about May 17, 2017 to May 25, 2017, defendant and his co-conspirators exfiltrated or transferred documents from Company A's computer network.

f. On or about May 24, 2017, defendant and his co-conspirators accessed Company A's computer network with the login and password assigned to Individual J.N.

All in violation of Title 18, United States Code, Section 371.

COUNT FOUR

The SPECIAL MAY 2021 GRAND JURY further charges:

1. Paragraphs 1(a) through 1(e) of this indictment is incorporated here.

2. Between on or about March 2, 2017, and on or about May 25, 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

defendant herein, intentionally accessed a computer used in interstate and foreign commerce without authorization and exceeded authorized access and thereby obtained information from a protected computer, namely the computer network of Company A, and (1) the offense was committed for purposes of commercial advantage; (2) the offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud; and (3) the value of the information obtained exceeds $5,000;

In violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i), (c)(2)(B)(ii), and (c)(2)(B)(iii).

COUNT FIVE

The SPECIAL MAY 2021 GRAND JURY further charges:

1. Paragraphs 1(a) through 1(e) is incorporated here.

2. On or about March 14, 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

defendant herein, knowingly possessed, and used, without lawful authority, a means of identification of another person, namely, Individual J.Y.'s Company A username and password, during and in relation to a felony violation, namely an offense under Title 18, United States Code, Section 1343, as described in Count One of this indictment, and Title 18, United States Code, Section 1030, as described in Count Four of this indictment, knowing that the means of identification belonged to another person;

In violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT SIX

The SPECIAL MAY 2021 GRAND JURY further charges:

1. Paragraphs 1(a) through 1(e) is incorporated here.

2. On or about May 24, 2017, in the Northern District of Illinois, Eastern Division, and elsewhere,

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"

defendant herein, knowingly possessed, and used, without lawful authority, a means of identification of another person, namely, Individual J.N.'s Company A username and password, during and in relation to a felony violation, namely an offense under Title 18, United States Code, Section 1343, as described in Count Two of this indictment, and Title 18, United States Code, Section 1030, as described in Count Four of this indictment, knowing that the means of identification belonged to another person;

In violation of Title 18, United States Code, Section 1028A(a)(1).

FORFEITURE ALLEGATION

The SPECIAL MAY 2021 GRAND JURY further alleges:

1. Upon conviction of an offense in violation of Title 18, United States Code, Section 1030(a)(2)(C), as set forth in this Indictment, defendant shall forfeit to the United States of America:

a. any property constituting and derived from proceeds obtained directly and indirectly as a result of the offense, as provided in Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B); and

b. any personal property used and intended to be used to commit and to facilitate the commission of the offense, as provided in Title 18, United States Code, Section 1030(i)(1)(A).

2. Upon conviction of an offense in violation of Title 18, United States Code, Section 1343, as set forth in this Indictment, defendant shall forfeit to the United States of America any property that constitutes and is derived from proceeds traceable to the offense, as provided in Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

3. The property to be forfeited includes, but is not limited to:

a. a personal money judgment in an amount equal to the proceeds derived from the offenses in violation of Title 18, United States Code, Sections 1028A, 1030(a)(2)(C), and 1343;

4. If any of the property described above, as a result of any act or omission by a defendant: cannot be located upon the exercise of due diligence; has been

transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property, as provided by Title 21, United States Code Section 853(p).

A TRUE BILL:

_____

FOREPERSON

_____

Steven J. Dollear on behalf of
JOHN C. KOCORAS
Attorney for the United States,
Acting Under Authority Conferred by
28 U.S.C. § 515

Exhibit A

JIA WEI (贾 伟),
also known as "chansonJW," "JWT," "JWT487,"
"asmikace," "asmikace3d," "askikace3d," and "haber william,"