United States of America

Applicability of Articles 6-16 to Modern Cybercrime

The proposed Draft text of the Convention (DTC) uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies. The core offenses currently in the DTC in Articles 6-16 enjoy consensus and are sufficient to cover a wide range of criminal activity, including many of the harms raised by those seeking additional criminalization provisions. This paper highlights how the existing provisions which enjoy consensus can be transposed to national law to address ransomware; terrorist attacks on computer systems; attacks on critical infrastructure; the provision of online services intended to aid and abet criminal conduct; the theft of personal data; the use of forged data; and the illicit use of payment instruments. In many cases, more than one Article may apply to the offense conduct. The United States is confident that cooperation against these harms can be achieved under the limited list of crimes in the proposed draft Treaty which already enjoys widespread

support and encourages the Committee to use the limited time remaining to achieve similar consensus on other chapters of the Convention.

Cyber-dependent and cyber-enabled provisions

Article 6 – Illegal Access

Access without right, i.e. without authorization from the resource owner, is the most basic computer offense and similar to trespass. Member states are free to qualify the meaning of "without right" or require additional elements such as the circumvention of a security measure or the copying of information. Any unauthorized access constitutes a crime under this provision, no matter its target or motivation, though Member States may choose in their own domestic systems to impose enhanced penalties for illegal access to critical infrastructure, non-public government systems, or systems holding personal data or national security information, or for terrorist purposes. The wide definition of illegal access under this treaty, without limitation to any particular systems or sets of data, ensures that Member States will be able to cooperate with each other on the full range of unauthorized intrusions, including ransomware, those committed in attacks

on critical infrastructure, terrorist attacks, and thefts of personal data. And access with right, including authorized pen testing or protection activities agreed to by the actor and resource owner, would not be a criminal act under this provision.

Article 7 – Illegal Interception

This Article criminalizes the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. Member states may also require dishonest intent or that the offence be committed in relation to a computer system that is connected to another computer system. This Article protects the privacy of data in transit within a computer system or communications through the Internet. In modern cybercrime, this is often achieved through the placement of malware or “sniffers” on a system to capture communications leaving that system, including bank logins, credit card, health or other sensitive data. Thefts of any data committed in this manner would constitute criminal acts of illegal interception, eliminating the need to

define specific categories of protected information under the terms of the treaty. As with the other provisions, Member States may choose in their domestic law to impose enhanced penalties for the illegal interception of certain communications or from certain systems, but Member States will be able to cooperate together against the full range of illegal interception crimes under the terms of the treaty. And as with illegal access, interception with right, including authorized pen testing or protection activities agreed by the actor and resource owner, would not violate this provision.

Article 8 – Data Interference

This Article criminalizes the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right. “Damage” or “deterioration” relates to changes to the integrity or content of data and applications. ”Deletion" of data is the equivalent of the destruction of a corporeal thing. “Suppression” of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. “Alteration" means the modification of existing data. Malicious software

code, such as viruses, Trojan horses, and ransomware are covered under this paragraph, as is the resulting modification of the data. Again, any such interference without right of the integrity of data constitutes a crime under this provision, no matter the characteristics of the data or system or the motivation of the unauthorized person. While individual states may seek to impose further penalties for damage to particular sets of sensitive data, the breadth of this Article ensures that Member States will be able to cooperate against data interference in any context under the terms of the treaty, including in situations involving terrorism, critical infrastructure data, or personal data.

And, again, these acts are only punishable if performed "without right." Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for testing or protection of a computer system authorized by the owner or operator or the changes made to a system by authorized software updates, are not crimes under this provision. Member states may also choose to exclude from criminal liability

altogether, or impose a lower penalty, if the culpable conduct does not cause serious damage as defined by national law.

Article 9 – System Interference

The provision criminalizes the intentional hindering of the lawful use of computer systems including telecommunications facilities, which prevent the computer or telecommunication systems from functioning properly. The text is formulated in a neutral way so that each member state may determine for itself the criteria for hindering to be "serious." For example, a member state may require a minimum amount of damage to be caused for the hindering to be considered serious. “Serious" could include denial of service attacks or ransomware attacks that have a significant detrimental effect on the ability of the owner or operator to use the system or to communicate with other systems. “Serious” could also relate to the kind of system hindered, such as a critical infrastructure system, or the motivation for the hinderance, such as for terrorist purposes. And, as with Articles 6-8, hinderance with right, even if serious, is not a violation.

Article 10 – Misuse of Devices

Trafficking in access devices is thriving in criminal markets. The Article criminalizes the sale, procurement for use, import, distribution or other acts making available of computer passwords, access codes, or similar data by which computer systems may be accessed or access to computer systems may be facilitated. This provision covers trafficking in passwords and other credentials, including banking credentials, with the intent of providing unauthorized access to a system, illegally intercepting data, or interfering with data or a system without right. As with the other provisions, the broad scope allows Member States to cooperate against the misuse of devices in a wide range of contexts, including ransomware, unauthorized access or interference with critical infrastructure, illegal interception of or access to personal data, and in furtherance of illegal access, interception, or interference with data or systems by terrorists.

Article 11 – Computer Related Forgery

This Article criminalizes fraud which relies on false data through the input, alteration, deletion, or suppression of computer data, without right, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. Although Article 12 will also cover this conduct, Article 11 by its terms requires the falsification of data with the intent that the data be considered authentic for legal purposes. As such, this Article can cover fraudulent documents used for identity theft by filling possible gaps in criminal law in traditional forgery statutes which may not apply to electronically stored data.

Article 12 – Computer Related Fraud

This Article criminalizes causing loss of property to another person by an input or alteration of computer data, or any interference with the functioning of a computer system with the fraudulent intent to procure an economic benefit for oneself or another person. Therefore, it applies to fraud committed through computers with either fraudulent input to

computer data or interference with a system if done with an intent to defraud and will cover all fraudulent schemes committed through the Internet. This Article authorizes member states to criminalize scams of all types for which a computer is used to commit fraud.