A Collective Initiative to Sustain the Growth of Our Global Digital Economy

The digital economy can be calculated as the share of total economic output derived from a number of broad inputs, such as digital infrastructure (hardware, software and communications equipment), digital skills, and the intermediate digital goods and services used in production. A recent study by Accenture Strategy and Oxford Economics values the United States' digital economy in 2016 at $5.9 trillion dollars (a third of US GDP) and an earlier report suggested that the digital economy could add $1.36 trillion to the GDP of the world's top ten economies by 2020 (the equivalent of adding another South Korea to the world economy).[1]

To protect our digital ecosystem, industry's dedication to security must equal its passion for innovation. The Council to Secure the Digital Economy (CSDE) will engage in a common effort across the Information, Communications and Technology (ICT) segments to assess threats to the expanding digital ecosystem and drive collective solutions, framed through a shared digital economy lens. Ultimately, through engaging a diversity of views across key ICT stakeholders, CSDE will produce more robust analyses and effective solutions to strategically address these critical issues.

CSDE has identified two initial projects that will demonstrate the effectiveness of a coordinated cross-sector effort to enhance our collective ability to prepare and respond to what is widely regarded as a critical, ecosystem-wide cybersecurity threat: botnets and other automated, distributed attacks.[2] The first project will produce an international guide of anti-botnet

[1] Mark Knickrehm, Bruno Berthon and Paul Daugherty. "Digital disruption: The Growth multiplier." Accenture Strategy. 2016. Accessed July 27, 2017. https://www.accenture.com/_acnmedia/PDF-4/Accenture-Strategy-Digital-Disruption-Growth-Multiplier.pdf

[2] "Botnets are networks of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes." CSRIC III, WG-7 Anti-Botnet Code of Conduct. 2012. Accessed May 1, 2018. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

baseline security practices for global ICT segments. A second initiative will create an operational framework for mobilization of the enabling organizations across the ICT sector that can convene rapidly to mitigate a major botnet/distributed attack.

Both of these projects build on previous foundational work that will be reviewed and updated as appropriate. Moreover, every effort will be made to ensure that CSDE activities complement ongoing efforts in various global venues to avoid unnecessary duplication of effort.

Develop and Promote International Anti-Botnet Guide for the ICT Sector

Problem Statement:

Every single day, more than a billion dollars is lost to the world economy because of cybercrime, much of which is accomplished via botnets. The threat that botnets and other automated, distributed attacks pose to the Internet and communications ecosystem has increased dramatically over time; more systems are vulnerable today than in any previous period of the Internet's history.

Malicious actors, including some nation states, use botnets and distributed attacks for a variety of nefarious purposes, including to overwhelm network resources; perpetrate scams and identity theft; steal sensitive personal information and intellectual property; spread infectious malware; defraud advertisers and other businesses; and even hold computer systems hostage for ransom. Like-minded governments throughout the world have called upon industry to take more aggressive action as part of a collective defense strategy.

The Council to Secure the Digital Economy (CSDE) members collaborate in this global effort to mitigate botnet attacks and other distributed attacks by implementing and promoting proven cost-effective solutions. However, the long-term security and resilience of the Internet and communications ecosystem requires a global and holistic approach that involves the adoption of baseline security practices by stakeholders in many different countries, industries, and segments of the ecosystem. CSDE will actively engage with global government and industry partners to enhance the transactional integrity of the underlying digital economy.

Project:

CSDE will develop and promote a guide to anti-botnet baseline security practices for global ICT segments. To inform this guide, CSDE will analyze global practices to address the threat that botnet/distributed attacks pose to the resilience of the Internet and communications ecosystem.

Action 1. Develop a compilation of effective technologies, tools, and common practices that have been shown to prevent and mitigate botnets and other distributed attacks.

Action 2. Produce an international anti-botnet guide of best practices related to education, detection, notification, remediation and collaboration for major ICT segments.

Action 3. Share the best practices with a broad spectrum of national and international stakeholders who are well-positioned to promote the Anti-Botnet Guide and further constructive engagement.

Impact Statement:

CSDE's anti-botnet guide will engage the international stakeholder community in a united effort to dramatically reduce destructive botnet attacks. By establishing a common taxonomy aligned with baseline security practices, each segment can focus on segment-specific guidance that can drive observable and measurable security improvements. To the extent that the practices are adopted widely throughout the ecosystem, the threat of botnets can be significantly diminished.

Mobilize ICT Against Major Botnet Attacks and Other Distributed Attacks

Problem Statement:

The evolving landscape of cyber threats, in particular botnets and other distributed attacks, poses global and ecosystem-wide economic security challenges, and in some instances may constitute a significant danger to human health and safety.

In the most severe scenarios, these challenges will exceed the individual response capabilities of any single company or industry, necessitating efficient coordination among ICT enablers and other relevant stakeholders to respond to high-level threats. CSDE's members have demonstrated exemplary leadership in the struggle against botnets and other distributed attacks by developing and improving methodologies to share threat information with relevant actors. Public and private sector partners have welcomed such advances, which form the basis of important working relationships throughout the world premised on shared security goals.

However, as of yet, there is no globally accepted operational framework to support rapid mobilization of critical private sector assets that may need to be leveraged to effectively respond and/or recover in the event of a major cyber emergency. Such emergencies may include threats to critical infrastructure, widespread Internet and communications ecosystem disruption, or some other mitigatable crisis that rises to the level of national or international significance.

Project:

CSDE will create an operational framework for mobilization of the ICT sector designed to mitigate a major botnet/distributed attack. CSDE will identify scenarios and thresholds where the event is sufficiently widespread to trigger ICT enabler coordination and will undertake activities to improve response capabilities.

Action 1. Conduct pre-planning activities to identify trigger thresholds, which determine whether a botnet scenario is sufficiently serious to justify ICT enabler activation, and identify the relevant enablers.

Action 2. Develop pre-scripted mitigation strategies, with playbooks for different scenarios to guide industry action.

Action 3. Test and implement pre-scripted mitigation strategies and playbooks, including coordination with relevant government entities/officials.

Impact Statement:

In the event of a catastrophic cyber incident, a unified operational framework for mobilization of the ICT sector is essential to coordinate flexible response mechanisms and distribute responsibilities among stakeholders with clearly defined leadership roles during a major incident.

The goal is to convene the appropriate set of stakeholders who are best positioned to take the immediate steps necessary to mitigate severe harms caused by distributed attacks.

This framework would streamline industry and government actions in the event of major cyber emergencies, so that precious time is not lost on non-essential, low-priority activities.