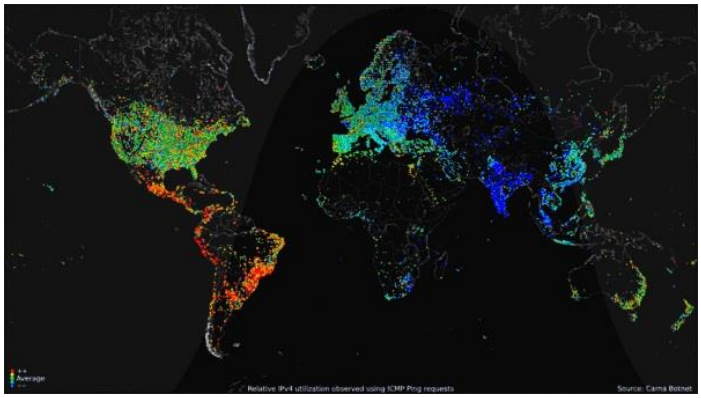
SCENARIO #5: **#OpJustina: DDoS Attack**

Scenario:

Multiple distributed denial-of-service (DDoS) attacks hit Boston Children's Hospital over the weekend of April 19, 2013. The attacks knocked the hospital offline for days, which was enough to critically disrupt the hospital's day-to-day operations and its research capabilities [1]. The attacks were part of #OpJustina, a campaign of the Anonymous hacker collective and aimed to raise public interest in the case of Justina Pelletier, a young girl who was separated from her parents after a (mis)diagnosis made by Boston Children's Hospital medical staff. The main figure of the attacks, Martin Gottesfeld, was arrested in 2016, and sentenced on January 10, 2019 to ten years in prison [2]. He was also ordered to pay $443,000 in restitution for damages caused by his DDoS attacks, which he allegedly carried out with the help of a "botnet" made up of over 40,000 internet routers [3]. See the figure on the right for an earlier example botnet. Effective defenses are extremely difficult to design because the traffic volume generated by a DDoS attack can exceed the capacities of most corporate Internet links, the attack packets come from many sources and can be geographically distributed, which makes IP source traceback extremely difficult, and the traffic from each attack source tends to appear "legitimate" [5].



An earlier example botnet called the Carna botnet [4]. It was a botnet of 420,000 devices created by an anonymous hacker in 2012. It didn't have any intentions on doing anything malicious; in fact, it showed us what the Internet looked like. But of course it demonstrated the security vulnerability.

Students will learn the inherent design features of the Internet which created the potential for different types of DDoS attacks and defense mechanisms, and countermeasures against these defenses [5, 6]. Test of this scenario is consisting of two phases, first looking for vulnerable systems available in the Internet and installing attack tool in these compromised systems (bots) and second sending an attack command to the bots through a secure channel, for example Internet Relay Chat (IRC) channel, to launch a bandwidth attack against the targeted victim(s) [5]. Note that the packets in the attack traffic may use a fake source IP address in order to make it harder for the target of the attack to identify the source of the attack traffic. Students will implement the second phase, i.e., a small-scale DDoS attack scenario, on the VirtualBox environment. (Advanced students may want to explore alternative test platforms such as Mininet [7], OpenStack [8] and DETER [9].) The attack will be a "volumetric attack" which attempts to create congestion by consuming all bandwidth available to the target.

Students will also review the applicability of the Computer Fraud and Abuse Act (CFAA) and examine whether that law should be updated to address these newer cybercrimes. Note that the CFAA law was written three decades ago to protect government computers from "unauthorized

access." There were several controversial cases including Aaron Swartz (2013) and Lori Drew (2008). Also, they will discuss on the bounds of protest in the digital age.

For your information, here is the Justina's story in more detail: According to her family, Justina had been receiving treatment for mitochondrial disease at Tufts Medical Center. When she came down with the flu, Tufts doctors advised Justina's parents to take her to Boston Children's Hospital. There, Dr. Newton decided that Justina had been misdiagnosed. She really had somatoform, a psychiatric disorder that causes physical ailments, the physician decided. Her parents protested a plan to remove Justina from her treatments for mitochondrial disorder in favor of psychiatric treatments. When they tried to discharge her to take her back to Tufts, they were faced with a 51A – a report of alleged child abuse or neglect.

NICE Workforce Framework for Cybersecurity:

Scenario #5 & #6 will cover the following Knowledge areas.

K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0004 Knowledge of cybersecurity and privacy principles.
K0005 Knowledge of cyber threats and vulnerabilities.
K0007 Knowledge of authentication, authorization, and access control methods.
K0013 Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0046 Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0070 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0116 Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0131 Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0135 Knowledge of web filtering technologies.
K0202 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0210 Knowledge of data backup and restoration concepts.
K0373 Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0392 Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0452 Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0624 Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

References:

[1] The Hacker Who Cared Too Much, https://www.rollingstone.com/culture/culture-features/the-hacker-who-cared-too-much-196425/

[2] Anonymous hacker gets 10 years in prison for DDoS attacks on children's hospitals, https://www.zdnet.com/article/anonymous-hacker-gets-10-years-in-prison-for-ddos-attacks-on-childrens-hospitals/
[3] Anonymous takes on Boston Children's Hospital in #opJustina, https://news.sophos.com/en-us/2016/10/24/anonymous-hacker-charged-with-opjustina-ddos-attacks-on-hospitals/
[4] https://en.wikipedia.org/wiki/Carna botnet
[5] T. Peng, C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, Vol. 39, No. 1, April 2007.
[6] DDoS Attack, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[7] Mininet: An Instant Virtual Network on your Laptop (or other PC) - Mininet. http://mininet.org/
[8] OpenStack. Home - OpenStack Open Source Cloud Computing Software, https://www.openstack.org/
[9] DETER Project, https://deter-project.org/