Cyber Security Is Not Censorship[1]

Dorothy E. Denning
Naval Postgraduate School

November 19, 2013

Many cyber security mechanisms block access to and the flow of information. Firewalls, for example, stop the flow of selected packets to and from a network. Intrusion prevention systems and anti-virus tools block packets and software that match the signatures or behavior of malicious ones. Access controls, user authentication, and cryptography prevent unfettered access to systems and information. Flow controls prevent information from flowing from objects at one classification level to those at a lower level.

Because the mechanisms used for censorship also block access to and the flow of information, cyber-security might be seen as just a form of censorship. In this essay, I will argue that it differs from our common understanding of censorship in three important ways.

First, cyber security is more about the execution of code than information in a passive or inert sense. The reason that firewalls and intrusion prevention systems block certain packets entering a network is that the packets could trigger the automatic execution of code whose effects would be harmful. In particular, the packets might contain malicious software (malware) that would be executed upon arrival or malicious input data to programs that process the incoming packets. Similarly, anti-virus tools stop viruses and other forms of malware from running on the systems they reach. It isn't that the virus code is dangerous to look at; rather, the danger comes from its execution. Access controls and user authentication mechanisms do more than just keep users away from certain data – they keep users from running code against the data in order to exfiltrate or download the data, or to modify or delete it. Even security mechanisms that prevent outgoing flows of data are as much about code as data. For example, a firewall rule that blocks packets whose destination IP address matches that of the "drop server" used by malicious exfiltration code would not be needed if other security mechanisms could keep the malicious code off the network. Denial of service (DoS) and distributed DoS (DDoS) attacks are also about code. Although the immediate concern may be resource capacity, owing to the sheer volume of traffic, these attacks would not be a threat were it not for the code that drives them (e.g., to command a botnet to send out gigabits of traffic per second) and is often exploited by them (e.g., to amplify effects through DNS reflection).

By contrast, censorship is about blocking information from human eyes and ears on the grounds that people receiving the information might be harmed in some way or use the

[1] Approved for public release; distribution is unlimited. The views expressed in this document are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

information in a way that it harmful to the censor's objectives. Here the concern is not with the execution of software, but rather with what humans might do with the information. This distinction is apparent when one considers that computer crime laws generally allow the publication and distribution of malicious software for human viewing, but not for the purpose of triggering computer infections. For example, it is permissible to post virus or exploit code on a research website, but not to launch the virus or use the exploit to gain access to a system without authorization.

The second way that cyber security differs from censorship is that the former is concerned with the volume of data as well as its content. This is particularly true in the case of DoS and DDoS attacks. Whereas a single webpage request (i.e., HTTP GET packet) to a public-facing server usually poses no cyber-security threat, a flood of billions of such requests does, and so might trigger controls to block the packets. Attacks that employ network scanning to find open and vulnerable access points can also trigger security controls that respond to the volume of traffic. By contrast, censorship controls are generally not concerned with volume; if they would allow a single request for a webpage, they would allow a billion.

The third way cyber security differs from censorship is that security controls serve to protect systems and their data from cyber-attacks, whereas censorship serves to protect populations from exposure to material deemed harmful, say because it is believed to threaten social norms or stability, national security, or political power. Further, the owners of cyber resources choose which security controls to deploy based on their expected needs and risks from cyber-attacks. Certain industries may be required by law to install particular security controls (e.g., to protect financial or health records), but these mandates are generally consistent with industry objectives to protect their information and that of their customers and clients.

By contrast, censorship is more about third party, particularly government, mandates and controls that have little if anything to do with preventing cyber-attacks and may or may not be desired by those subject to the controls. Under censorship, an information flow from one person to another may be blocked not because either party wants that to happen, but because the state has forbidden it. The state may implement some of the controls, say by installing packet filtering mechanisms in backbone routers that are owned and operated by the state. The state may also direct private-sector entities such as web hosting companies, private ISPs, search engine providers, and cyber cafes to implement the controls.

Censorship meets cyber security when the same blocking technologies are used for both. For example, a network owner might filter out some packets because of censorship rules from the state and others because they are known to be associated with DDoS or other types of cyber-attacks that are affecting the network or its customers. Censorship also meets cyber security when security controls intended to block cyber threats have the side effect of also stopping non-threatening flows. For example, a company might block employee access to certain websites on the grounds that malware was found on the sites, but in the process effectively censor other content hosted on the sites. Still, even though

blocking technologies play this dual role, cyber security and censorship have different objectives and concerns. Cyber security aims to defend against cyber-attacks and is concerned with executable code and traffic volume as well as information content; censorship aims to defend against more general harm and is concerned almost exclusively with content and its impact on human populations.