MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

RESEARCH SUMMARY

ACTIVE DEFENSE
An Overview of the Debate and a Way Forward

With the growth of information technology, major businesses face an increased risk of hacking and data breach. In recent years Target, Home Depot, JPMorgan Chase, and Sony, to name only a few, have suffered attacks at the hands of nefarious technology intruders. While businesses may protect their own networks from intrusion, there are questionable legal implications involving "active defense" or fighting back by disrupting or destroying the attacker's network or server.

A new paper for the Technology Policy Program at the Mercatus Center at George Mason University demonstrates it is more efficient for businesses to engage in active defense—also called "hacking back" or "counterhacking"—than to rely on the government to solve the problem. Businesses should be free to use the technological resources at their disposal to protect themselves and their consumers, while being subject to strict liability in the event of unreasonable countermeasures against an innocent party unrelated to the attacker.

To read the paper in its entirety and learn more about its author, Anthony D. Glosson, see "Active Defense: An Overview of the Debate and a Way Forward."

TYPES OF ACTIVE DEFENSES

Active defenses in information technology involve more than hardening one's own network; they include countermeasures that seek to unmask an attacker or disable the attacker's system. Active defenses can be broken down into two categories outside of one's own network.

- *Observation and access:* Victims of hacking can use different tools to help identify the attacker and deduce the attacker's motive. Victims can also view their attacker's files, map its resources, and gather evidence for authorities.
- *Disruption and destruction:* Victims of hacking can deflect traffic toward the attacker and try to crash the attacker's system. Victims can also delete files, change the attacker's

For more information, contact
Kate De Lanoy, 703-993-9677, kdelanoy@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor, Arlington, VA 22201

passwords, or even remotely break the attacker's system so that it cannot harm the victim or anyone else unless the attacker expends time and effort repairing it.

LEGAL AND POLICY DEBATES OVER ACTIVE DEFENSE

Some question whether businesses violate the law if they engage in certain types of active defenses, especially disruption and destruction. The Computer Fraud and Abuse Act (CFAA) prohibits accessing another computer without "authorization" to do so.

- *The CFAA imposes a barrier to active defense*. While no court has yet ruled on what would be a novel legal question, it seems likely that the simple answer—that a business does not have authorization to access or delete an attacker's files—would be adopted by the courts under the CFAA.

- C*ommon law legal defenses may help but are unreliable*. While it is possible that a court could accept common law defenses like the privilege to use reasonable force to protect one's possessions, such murky and complex reasoning is unlikely to encourage businesses to risk legal consequences to protect themselves.

- *Active defense is proven to work*. For example, in 2009 a group of Chinese hackers attempted to appropriate Google's account login technology. In response, Google security teams compromised a server used by the hackers that contained evidence and shared it with law enforcement and intelligence authorities. Enabling law enforcement to share information with businesses to secure the Internet is likely to benefit consumers.

- *Businesses are better suited to engage an attacker*. Businesses employ security professionals, and they can spot anomalies better than government investigators and more quickly than the government. Government resources are already stretched thin, so placing the burden of identifying and deterring attackers on the government would be inefficient.

- *Businesses are currently incentivized to avoid government involvement*. Businesses may fear reporting unresolved breaches to the government as such reports could undermine consumer and investor confidence. In some cases, businesses have good reason to fear the Federal Trade Commission's strategy of prosecuting businesses that are victims of consumer data breaches.

POLICY PROPOSAL: RIGHT TO QUALIFIED ACTIVE DEFENSE WITH STRICT LIABILITY FOR MISDIRECTED ACTIONS

Congress should add a qualified right of active defense to the CFAA. This right would balance active defense privilege with misattribution concerns by imposing strict liability for harm caused during the use of misdirected active defense efforts. This policy would force those who invoke the right to active defense to internalize the costs of misattribution.

Legal Standard

To avoid liability, a defendant would need to prove that the plaintiff was the initial attacker or all of the following:

- The defendant's active defense measures were limited to observation and access; and
- the initial attacker was routing traffic through the plaintiff's network at the time of the active defense action; and
- obtaining the plaintiff's cooperation in tracing the initial attacker was impracticable.

Stiff Statutory Damages

Firms will likely engage in active defense when the value of doing so exceeds the risk of liability, so Congress should offset the problem of accurately attributing where an attack is coming from by imposing stiff statutory damages, creating an incentive structure that allows businesses to take risk when they determine doing so is efficient.

- As network security becomes a focus in the economy, insurers may offer coverage for liability incurred during active defense campaigns.

CONCLUSION

Policymakers should avoid unilaterally disarming victims from fighting back to protect themselves and the economy from criminals. There is an efficient and practical response to hacking: businesses should be allowed to engage in active defense to thwart hackers' attempts to harm them and others.