**BOFOX RESPONSE RECCOMENDATION**

**To:** National Security Council

**From:** CDT Joseph Zuccarelli, CDT William Nevils, CDT Michael Moore

**Subject: Deterrence by Denial of the “Bofox” Attacks**

**Date:** 25 November 2020

**Executive Summary: Recommendations**

* A massive denial of service attack on “Internet of Things” (IoT) devices hit major cities across the United States and Europe. The suspected threat actors involved in this attack are persons aligned with the U.S.-based Antifa movement.
* In response, the United States should immediately begin to work through BigFox, the private manufacturer of the IoT devices in question, to update the compromised devices and take steps to implement rigorous and legally binding standards for IoT devices used in critical infrastructure going forward.
* This proposed course of action would mitigate the effects of these attacks in the short term and deter future attacks by lowering their chance of success in the long term.

**Problem Statement and Strategic Considerations**

On December 18th, 2017, several major metropolitan areas across the United States and Europe were affected by a massive denial of service attack on IoT devices. Operations, devices, and associated users in the following cities have been affected by these “Bofox” attacks: New York City, San Francisco, Chicago, Paris, London, Berlin, Moscow. These attacks have propagated over Low-Power Wide Area Network (LWPAN) infrastructure installed and managed by a French company known as BigFox, SARL. The resulting impacts on critical infrastructure include disruptions to telecommunications and cellular networks, sporadic power outages, and disruption of electronic banking systems and commuter transportation systems. The DHS and FBI are attributing the attacks to persons aligned with the U.S. based Antifa movement. The attacks are currently still ongoing, and thus IoT devices using LWPAN infrastructure remain vulnerable. Given the complexity of the attacks, the attackers’ familiarity with the BigFox vulnerability, and their access to U.S.-based sensitive financial and critical infrastructure networks, the danger and likelihood of further attacks is high. Therefore, the National Security Council must coordinate a response that leverages all the resources of the United States Government.

**COA 1: Status Quo**

This is a laissez-faire approach, in which the council does nothing and critical infrastructure firms are responsible for developing their own security protocols in response to the attacks. There are several benefits of this approach. By doing nothing the council does not run the risk of improper attribution that would perhaps lead to a counterattack against the wrong threat-actor. This option also does not require any coordination with other nations or private organizations and can certainly be considered the cheapest option in the short-term. However, the potential consequences of choosing not to act in response to the attacks are too drastic. The attacks are still ongoing and thus IoT devices utilizing LWPAN infrastructure remain vulnerable. Deciding to do nothing in response projects weakness from the U.S. government, perhaps making the country susceptible to more attacks in the future.

**COA 2: Response to Terror**

The assumption that drives this course of action is that the cyber attack was conducted by an international terrorist group, rather than a domestic group like Antifa. Because many Western cities, as well as Moscow, were attacked, it is possible that a Middle Eastern or East Asian terror group was responsible. In response, the U.S. should engage in multilateral action to neutralize the threat actor responsible for this attack and other cyber-terrorists across the globe.

Immediate action in this COA requires the U.S to enroll in the Comprehensive Convention on International Terrorism (CCIT) and to prioritize funding for the FBI and DHS. Since the attack involved cells in both the U.S and Europe, the U.S should join a multilateral institution capable of enforcing justice across sovereign nations. Allocating funding towards domestic institutions will assist in locating the cells within the United States. Aggressive action should be taken to expand on the signal lead from New York City and to conduct denial attacks on terrorist news networks, such as Amaq News. This is also including kinetic strikes on terrorist leaders and facilities. Denying their ability to claim responsibility for the attack will deny them of their prize, fear, and thus inhibit their desire to conduct future attacks. Long term strategy under this course of action involves cooperation between the U.S and member partners of the CCIT to develop mechanisms for targeting and neutralizing cyber terror actors.

The advantages of this COA are that threat actors will be afraid to launch attacks because they are more likely to be caught and punished. Additionally, burden sharing through international cooperation will reduce the required U.S. expenditure on cybersecurity. Despite these strengths, treating the attackers as an international terrorist organization as opposed to a state actor, there is a high risk of misattribution and efforts being wasted on the wrong target. A retaliation that fails due to misattribution could serve to embolden other threat actors.

**COA 3: Deterrence by Denial**

Without confident attribution, deterrence by punishment and ostracization due to violation of norms are not feasible options.[[1]](#footnote-1) Because we don’t know the identity of the attacker, it’s difficult to tell whether deterrence by entanglement a valid approach is either.[[2]](#footnote-2) Therefore, this approach is focused on deterrence by denial. By prioritizing a quick and robust defense of the networks that the United States’ critical infrastructure relies upon, we minimize the effects of the current attack and deter future cyber-attacks by lowering their probability of achieving the intended outcome.

In terms of immediate action, we recommend that ICS-CERT, CISA, and CYBERCOM be directed to provide resources and technical expertise to assist BigFox in performing a global update of their devices. If BigFox is unwilling to comply, the DOJ should be prepared to take legal action to force their compliance. In the long term, the CISA and the DOJ should be directed to establish a formal mechanism for rapidly enforcing and performing similar updates on critical infrastructure devices should a similar attack occur in the future. Additionally, CISA must receive additional funding to expand its penetration testing capabilities for IoT devices. Finally, the existing institution of the NIST Framework should be expanded upon to include additional guidelines developed from CISA pen-testing, and adherence to the NIST Framework’s standards should become mandatory for private companies involved in critical infrastructure.

The benefits of the deterrence by denial approach are that there is no risk of escalation or embarrassment from retaliation against the wrong threat actor. Additionally, this strategy will be implemented faster than a multilateral strategy, as it does not require time-consuming diplomatic negotiations. The disadvantages of this course of action are that the lack of explicit deterrence via retaliation may embolden future threat actors and cyber defense against state-sponsored APTs will likely never be perfect. Additionally, cyber defense is typically more expensive, so this course of action will most likely impose significant costs on both the federal government and the private sector. Finally, a failed global update could have unpredictable repercussions.

**Policy Recommendation: COA 3**

We recommend pursuing COA 3: Deterrence by Denial. The status quo response projects weakness, thereby inviting future attacks, and the terrorist response is likely to fail without proper attribution. Deterrence by Denial projects strength without the risks associated with misattribution. Additionally, this approach has the greatest chance of mitigating the effects of the attack in the short term and, while a retaliatory attack based on questionable attribution may or may not dissuade future attacks, deterrence by denial will take concrete measures to reduce their probability and severity.

Works Cited

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/isec\_a\_00266.

1. Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace,” International Security 41, no. 3 (2017): pp. 52-62, https://doi.org/10.1162/isec\_a\_00266. [↑](#footnote-ref-1)
2. Nye, “Deterrence and Dissuasion in Cyberspace,” 52-62. [↑](#footnote-ref-2)