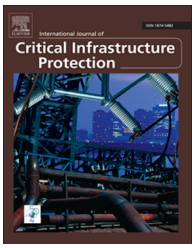
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



WikiLeaks and the risks to critical foreign dependencies

Daniel G. Arce

Department of Economics, University of Texas at Dallas, GR 31, 800 W. Campbell Road, Richardson, Texas 75080, USA

ARTICLE INFO

Article history:
Received 9 October 2014
Received in revised form
17 July 2015
Accepted 27 July 2015

Keywords:
WikiLeaks
U.S. Department of State
Critical Foreign Dependencies Initiative
Critical infrastructure
Risks

ABSTRACT

During its "Cablegate" campaign, the WikiLeaks website released a U.S. Department of State list of world-wide assets vital to the United States created under the Critical Foreign Dependencies Initiative (CFDI). This paper evaluates the entries in the CFDI list relative to various definitions of critical infrastructure pertaining to homeland security, and past patterns of terrorism attacks on categories within the CFDI as recorded by the Global Terrorism Database (GTD) over the past 40 years. It is found that what the United States identifies as critical international infrastructure differs significantly from what is defined as the national critical infrastructure. Moreover, the geospatial distribution of foreign infrastructure identified as critical by the United States differs substantially from the past patterns of terrorist attacks on similar entities. Finally, examining the GTD for the years subsequent to the WikiLeaks release reveals that there is little evidence to substantiate that WikiLeaks provided a "to-do" list for terrorists intending to attack critical infrastructure assets as was claimed by some U.S. government officials.

1. Introduction

During December 2010, the WikiLeaks website – founded by Julian Assange – released the U.S. Department of State secret Cable 09STATE15113 sent to then-Secretary-of-State, Hillary Rodham Clinton, which contained a list of worldwide assets vital to the United States. The list was created under the "Critical Foreign Dependencies Initiative," hereafter referred to as CFDI. The CFDI list was compiled by U.S. embassies and includes potential terrorism targets such as points of entry and rail crossings between the U.S. and Canada and between the U.S. and Mexico; dams and nuclear power plants that supply electricity from these two countries to the U.S.; private foreign companies across the globe in the areas of biotechnology, defense procurement, energy manufacturing and pharmaceuticals; a wide array of entities in the supply chain of natural gas and petroleum (export terminals, oilfields, pipelines, refineries and straits); select ports in Asia and Europe; and telecommunications assets such as transoceanic cable landings and satellite earth stations. The CDFI list, which is summarized in Table 1, has more than 200 individually-identifiable entities.

Opinions about the impact and risks associated with the WikiLeaks release of the CFDI list vary greatly. These range from claims that nothing new was revealed because information about the targets is publicly available to the U.S. government's condemnation of the release as a to-do list for terrorists. Cable 09STATE15113 itself asserts that if the assets on the list were to be destroyed, disrupted or exploited, there would be an immediate and deleterious effect on the United States. Assange's own rationale for releasing the CFDI cable was two-fold [7]:

> "To further show that U.S. diplomats were being illegally used to conduct foreign spying (it is explicitly stated in the cable to keep such inquiries secret from the host

E-mail address: darce@utdallas.edu

http://dx.doi.org/10.1016/j.ijcip.2015.07.004

Please cite this article as: D.G. Arce, WikiLeaks and the risks to critical foreign dependencies, International Journal of Critical Infrastructure Protection (2015), http://dx.doi.org/10.1016/j.ijcip.2015.07.004

Table 1 – Critical infrastructure assets in the CFDI list.

CDFI list entries	Sites
Biotech, chemical and pharmaceutical private businesses	43
Defense weapons/components private contractors	13
Electrical power generating sites	12
Energy component private manufacturers	14
Mining	19
Oil and gas production, storage and transportation	24
Points of entry into the U.S. (PoEs)	22
Telecommunications	28
Transportation and shipping	32
Total	207

government), and to reveal the "assets" the U.S. might fight a war over or otherwise use its diplomatic muscle to control."

In Hastedt's [16] taxonomy of the patterns of public intelligence, this statement corresponds to a promotional leak, which seeks to draw attention to oneself or to a policy problem. Moreover, the information contained in the CFDI list was not contested by the U.S. government. The direct release of the CFDI list by WikiLeaks itself was a one-time break within the context of WikiLeaks' pattern of diplomatic cable releases during 2010, known as "Cablegate." The large Cablegate cache (some 250,000 cables) was first released privately by WikiLeaks in tranches to news outlets such as *Der Spiegel*, *El País*, *The Guardian* (which passed them on to the *New York Times*) and *Le Monde* [6,7]. Once these outlets established the authenticity, veracity and sensitivity of the diplomatic cables, they published redacted versions that were deemed to be newsworthy. As Michael [24] notes, by late 2011, the unredacted cables were made available when the passphrase used to decrypt the cables was unintentionally made public by a reporter. Consequently, the cables are now downloadable as a searchable database.

The U.S. Department of Justice considered charging Assange with the crime of "communicating with the enemy," just as it charged U.S. Army Private Manning, who originally passed the cables to WikiLeaks. In July 2013, Private Manning was acquitted of this charge, but was convicted of lesser charges such as violations of the Espionage Act, using classified information for other than its intended purposes and theft of government property. In August 2013, Manning was sentenced to 35 years in prison.

In order to further limit the release of information potentially damaging to the U.S. by WikiLeaks, several restrictive measures were taken by private commercial entities apparently in response to unofficial exhortations by U.S. Senate Homeland Security Committee Chair, Joseph Lieberman: WikiLeaks' domain name provider dropped its service after a large-scale distributed denial-of-service attack on WikiLeaks; Amazon denied WikiLeaks access to its cloud-based web hosting service; Apple pulled a WikiLeaks app from its App Store; credit card companies and PayPal stopped processing donations to WikiLeaks; and INTERPOL issued notices seeking Assange for questioning in connection with rape charges in Sweden [7] (this revelation was itself a leak). Note that Benkler [7] maintains that there is no clear evidence that these acts were done at the direction of or coercion by a government official.

The vast majority of the academic literature on WikiLeaks considers the legality of the larger Cablegate cache of releases and the risks and ill effects of disclosing classified documents. Moreover, the candid assessment of conditions abroad in the cables caused considerable embarrassment and diplomatic difficulties for the U.S. and foreign governments. The consensus is that nothing new was learned from Cablegate, with the impact having to do with suspicions being confirmed via leaked official sources. At the same time, several experts surmise that the diplomatic cable assessments of Arab leaders had a role to play in the Arab Spring of 2011. Indeed, Bachrach [5] is among many who observe that the seeds of revolution in Tunisia were sown a month before the uprising via a WikiLeaks release of a dispatch by U.S. ambassador Robert Godec, which documented the greed and massive corruption of Tunisian president, Zine el-Abidine Ben Ali, and his family (also see [15]).

Prior to Cablegate, the WikiLeaks release of the Afghan War Diary raised concerns that reprisals would be enacted against persons identified in the reports. These concerns were seemingly validated by Taliban insurgents who threatened to decapitate the Afghan collaborators whose anonymity had been compromised by the publication of uncensored information from the Afghan War Diary [29]. Fenster [15] has used publicly-available media sources to establish that no individuals identified (or inferred) as U.S. intelligence sources or military or diplomatic personnel in the Cablegate documents have come to harm, although he does note that it is possible that such evidence exists in classified documents. Danielson [14] points out that Cablegate did result in the withdrawal of several U.S. diplomats as well as the resignation of the U.S. ambassador to Mexico. Hosenball [17] cites two U.S. intelligence officials as saying that they were aware of specific cases where the damage caused by Cablegate was assessed as serious to grave, although they could not discuss the subject matter because it was still highly classified.

Internal U.S. government reviews corroborate that Cablegate caused only limited damage to U.S. interests abroad [17]. Subsequently, in cooperation with the London-based Iraq Body Count, WikiLeaks created an automated program for redacting names within documents to minimize reprisals against human assets. WikiLeaks had been previously criticized for insufficiently redacting names in its release of the Afghan War Diary.

With respect to the CFDI list itself, left unaddressed are the issues of what was used to construct the list, what the list reveals about what the U.S. identifies as critical assets on foreign soil, and whether it can be used as a to-do list for terrorists, as has been claimed. This is the subject of the present paper.

In constructing the CFDI list, U.S. diplomatic missions needed to have a working definition of the critical infrastructure and past patterns of attacks on critical infrastructure assets. To this end, the CFDI list is compared with the more than 110,000 entries in the Global Terrorism Database (GTD) related to domestic and transnational terrorism incidents from 1970 through 2010, corresponding to the period prior to the

Please cite this article as: D.G. Arce, WikiLeaks and the risks to critical foreign dependencies, International Journal of Critical Infrastructure Protection (2015), http://dx.doi.org/10.1016/j.ijcip.2015.07.004