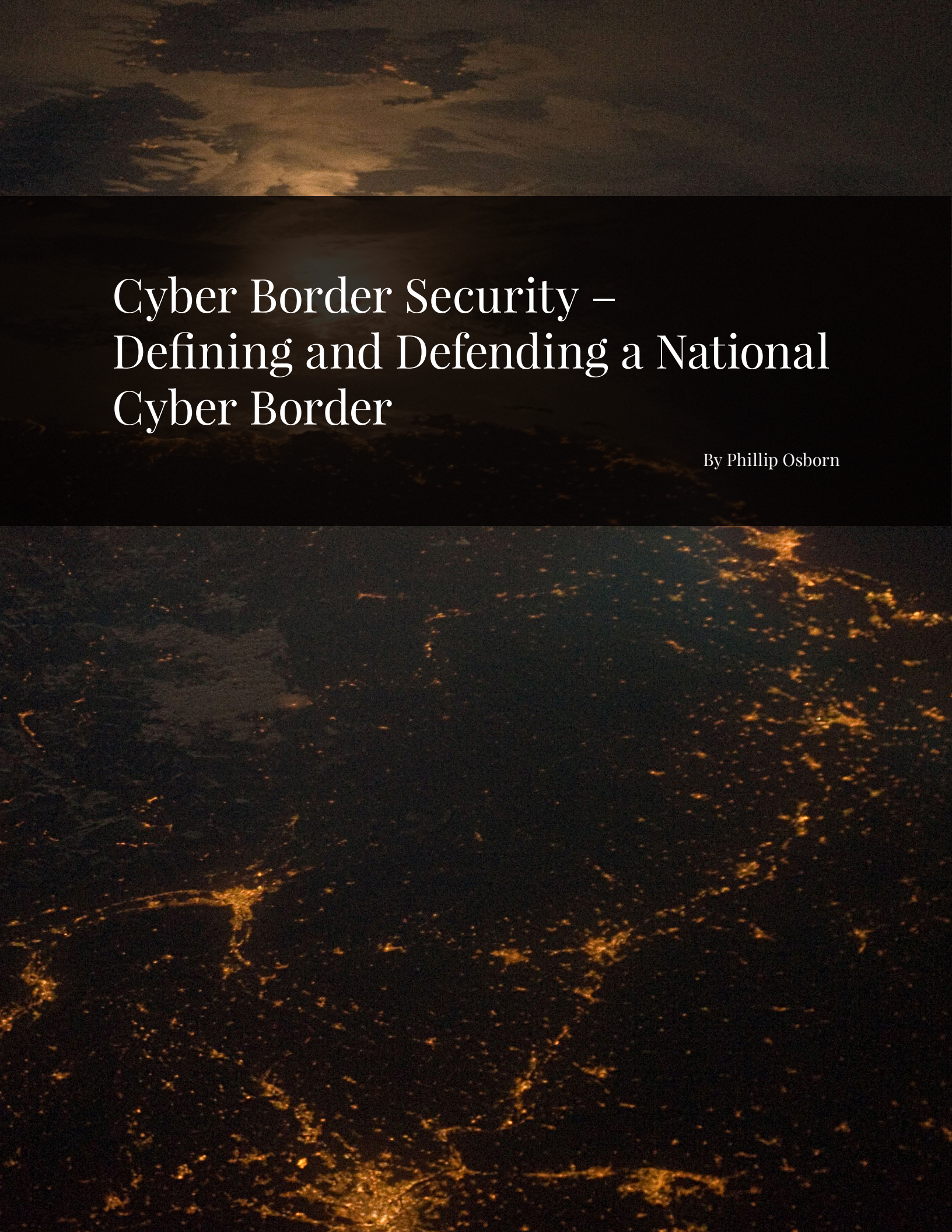


Cyber Border Security – Defining and Defending a National Cyber Border

By Phillip Osborn

Abstract

Concerns stemming from the convergence of border and cyber security threats are nothing new to those involved in both disciplines. Criminals and foreign actors have been exploiting computers and cyber methods to circumvent physical border security for decades. Today nearly every crime or homeland security threat that once required some physical nexus with the nation's traditional borders (land, sea, and air) is being committed, or at least facilitated, by some cyber component. In many ways vulnerabilities in cyber security render some aspects of traditional border security irrelevant, or at the very least, much less secure. The article explores this convergence of traditional border and cyber security and proposes a policy that would seek to evolve the concept of border security to include the cyber domain. Based on policy work begun over a decade ago by the author while the national cybercrime program manager for the U.S. Customs Service, the article details how a national cyber border can be defined and enforced. Relying on a methodology that adapts existing authorities, the article provides logical justifications and arguments for the need and legal authority to define a national cyber border. The strengths and shortcomings of this adaptive methodology are explored along with issues which may require new legislation. The article addresses some of the privacy concerns which are certain to arise from the cyber border concept using the same adaptive methodology of existing protections and expectations of privacy. The ultimate goal of the article is to stimulate thought- provoking discussion and spur further academic research into the convergence of cyber and border security; issues which are interdependent and clearly in the forefront of homeland and national security.

Suggested Citation

Osborn, Phillip. "Cyber Border Security – Defining and Defending a National Cyber Border." *Homeland Security Affairs* 13, Article 5 (October 2017). https://www.hsaj.org/articles/14093

Introduction

While the protection and control of our national borders has always been an important issue, the emergence of terrorist threats over the past several decades has brought concerns over border security to the forefront of national and homeland security discourse. A major topic in the 2016 presidential election contest, increasing border security became the central theme of the eventual victor and perhaps a strong indicator of the importance of the issue to a large portion of the electorate. Another less traditional security concern, but one that has rung alarms around the world, is the issue of cyber threats. Because of their asymmetrical nature and potential severity, cyber threats have become an overarching subject to national and homeland security interests. This document asserts that the two-- border threats and cyber threats-- are not mutually exclusive, and it explores the convergence of border and cyber security. Further, this article will show that the evolution of the concept of the border beyond the traditional land, sea, and air frontiers of the nation to include the cyber border is both inevitable and necessary. The article outlines the justification and conceptual framework for defining a national cyber border based on historical and traditional border analogies, and will discuss the existing legal framework that makes defining a national cyber

border possible, along with the authorities for protecting it. The purpose of this discussion is to introduce what at first may seem an exotic concept, and then to bring greater clarity and understanding of the subject to the researcher or homeland security professional. The article primarily focuses on defining the legal justifications for enforcing a national cyber border through the adaptation and interpretation of current and traditional U.S. border enforcement authorities. It leaves much of the "how" of policing it to the further academic and legal research that it hopes to stimulate. The following analogy is offered as food-for-thought regarding the cyber border and the debate for which this document hopes to be the catalyst. For hundreds of years, the distance of a cannonball shot was used to measure how far from shore a country should extend its legal control and territorial claims.[1] Leaders arrived at this distance based on the best technology of their day-- a cannon shot. This distance has changed and evolved over the years as newer technology made this original metric obsolete. We owe the founders of our country and the people of the nation our best attempt at interpreting the technologies of our day to develop policies and strategies to address the dynamic ways that cyberspace is changing the world and impacting national security.

The Convergence of Cyber and Border

What is border security and why is it so important? Simply put, the border is the point where foreign threats become domestic realities. The right and duty of government, is to control who and what crosses the nation's borders to protect the country and its people from foreign threats. The threats range from the obvious such as terrorists or criminals seeking to perpetrate an attack or commit a crime, to the less obvious such as contaminated agricultural and food products which could severely impact the nation's farming industry or sicken the populous. Because protection of the nation is such a compelling interest, border security is clearly viewed as a primary responsibility of the state. The traditional border security efforts of the government are obvious. Customs and Border Protection officers, Border Patrol Agents, and Coast Guard cutters are all physical measures employed to control the movement of persons and material entering, and in some cases exiting the country. These measures are a series of physical deterrents and inspection capabilities at the nation's boundaries to identify and control who and what is allowed to cross the border. The emergence of cyber threats however has radically changed the border security landscape forever.

The Internet and cyber methods provide an opportunity to circumvent traditional border security measures to perpetrate crimes and to harm the nation to a degree once only possible through large scale military actions. Terrorists, criminals, and nation states can and do take advantage of the asymmetrical nature of cyber methods to threaten and harm the nation and its people. Attacks on critical national infrastructure, the theft of sensitive government and industry trade secrets, the importation of hazardous and illegal materials, and the stealing of funds from banks and citizens are just a few of the crimes and threats that once normally required some physical compromise of traditional border security and controls to perpetrate. All of these actions are now possible by the illicit use of the Internet. Some crimes commonly committed against individuals by foreign actors today, like the theft of personal information or finances, would have been impossible or improbable before the advent of the new "cyber vector" of attack. Today cyber threats have converged with traditional border security threats and now either complement them, or provide new

opportunities to threaten the nation. By providing an avenue to circumvent physical border security measures, cyber methods have made many traditional border security efforts obsolete.

The Need to Define the Nation's Cyber Border

With cyber threats being such an obvious danger, one would assume that the government would take a similar responsible role in protecting the nation from foreign intrusions and threats, however this is not the case. Unlike traditional border security, the government's role in defending the nation from foreign cyber intrusion is far less robust. Rather than focusing on preventing the entry of cyber threats, the government functions in a response role, investigating after the fact and after an attack has occurred. Defense of the nation's cyber frontier is largely left up to private entities, both persons and organizations, to protect their own cyber borders. From a border security perspective this is highly undesirable due to interdependency issues since each individual or organization's computer or network once compromised can become an additional attack vector operating within the borders of our nation. This situation is analogous to making every individual responsible for their own physical border security, and ultimately that of the entire nation. Imagine the government conceding responsibility for land border security to the private land owners living along the border with little more than recommended best practices and advice on protecting their portion of the border. Imagine the responsibility for food and drug safety being left up to the individual consumers or businesses importing these goods. While this may sound absurd, this is essentially the situation in the government's approach to cyber threats.

One solution to the problem of foreign cyber threats is the evolution of the concept of the cyber border Once the concept of cyber border is defined, the government can use traditional laws and authorities to better protect the nation from current and future foreign cyber threats.

Borders in Cyberspace

An oft-repeated line is that in cyberspace there are no borders. This statement, while philosophically desirable among those seeking a more open world and society, is simply not true. There are physical borders that data transmission lines cross and there are functional equivalents of the border where data arrives directly from foreign places-- a very important concept that will be discussed further. The concept of borders in cyberspace even permeates computer network phraseology where terms such as "border routers" and "demarcation lines" are used to express the boundaries between networks. Yes, there are borders in cyberspace, we have just chosen not to acknowledge the cyber border as we do the land, sea, and air borders. Disruptive technologies which impact traditional border concepts are nothing new; the Internet is just the most recent. Air transport was another disruptive technology which required an evolution in traditional border security thinking and which provides an easy analogy to justify a similar evolution in the concept of the cyber border.

Disruptive Technologies and Border Security

The advent of air travel could arguably be judged as equal to or exceeding the Internet in the disruptive impact it has had on the world. Like the Internet, it has opened up opportunities for commerce and contact between peoples that would otherwise not exist. Like the Internet, air transport has also had a major impact on how war is waged, In terms of border security impact, air travel was also disruptive since there was no longer a traditional land or sea crossing at the countries' boundaries. Aircraft could fly across the borders and land deep within the country. The response to this was not to surrender border security and authority over what and who was entering the country via aircraft, but an adaptation and evolution in the definition of the border which allowed the exercising of traditional border authorities. The definition of the cyber border requires a similar adaptation and evolution in border thinking.

Defining the Cyber Border

Many current legal rulings and decisions regarding the Internet and Cyberspace are based on the interpretation of existing laws that govern conventional non-cyber circumstances. In many cases this methodology has succeeded in finding a workable application of existing laws, while in others, attempts at such an application have been cumbersome. Viewed in this light, the governance of cyberspace and the Internet may ultimately require some radical departure from contemporary legal thinking, perhaps a new separate U.S. Code crafted specifically for it. However, the legal framework to define the cyber border appears to be already present without any modifications or additions to existing laws.

Traditional Borders

The concept of traditional border— land, sea, or air—is relatively easy to grasp. Land borders are the geographic boundary separating the adjacent territories of other countries. The sea borders are a bit more complex and extend the physical border seaward from shore out to a specified distance. Currently this distance is 12 nautical miles seaward from the U.S. coast, increased from a 3 nautical distance which had been the distance claimed for many years. This claimed 12 mile zone is referred to as the territorial sea and is treated as the maritime border of the country. Additionally, the U.S. claims a further 12 mile nautical distance from the boundary of the territorial sea as Customs waters effectively allowing enforcement of customs and border controls seaward 24 nautical miles from the U.S. coast. Further, the U.S. claims an additional 200 mile seaward zone to enforce an economic, exploratory and exploitation zone which evolved from a 200 mile fishery conservation zone.[2] The variations and adjustments to border enforcement in the maritime realm are pragmatic and reflect the reality that time and technology necessitate changes and adaptations in order effectively to protect the nation. A similar adaptive view concerning enforcement of the air border discussed next, can also be used to define the cyber border.

The Air Border Analogy

The air borders are simply vertical extensions of the land and sea borders allowing control of the nation's airspace. As an aircraft enters U.S. airspace it is very much crossing the nation's border. Performing a Customs inspection of the aircraft, its passengers, and its cargo however would obviously be impractical at 35,000 feet. Where the aircraft lands therefore becomes what is referred to as the Functional Equivalent of the Border or FEB. The FEB is the first practical point where border controls can be exercised on the aircraft.[3] The clearest example of FEBs would be the foreign arrival areas of international airports where immigration and customs inspections of aircraft, passengers, and cargo are conducted well away from the actual physical border at its functional equivalent.

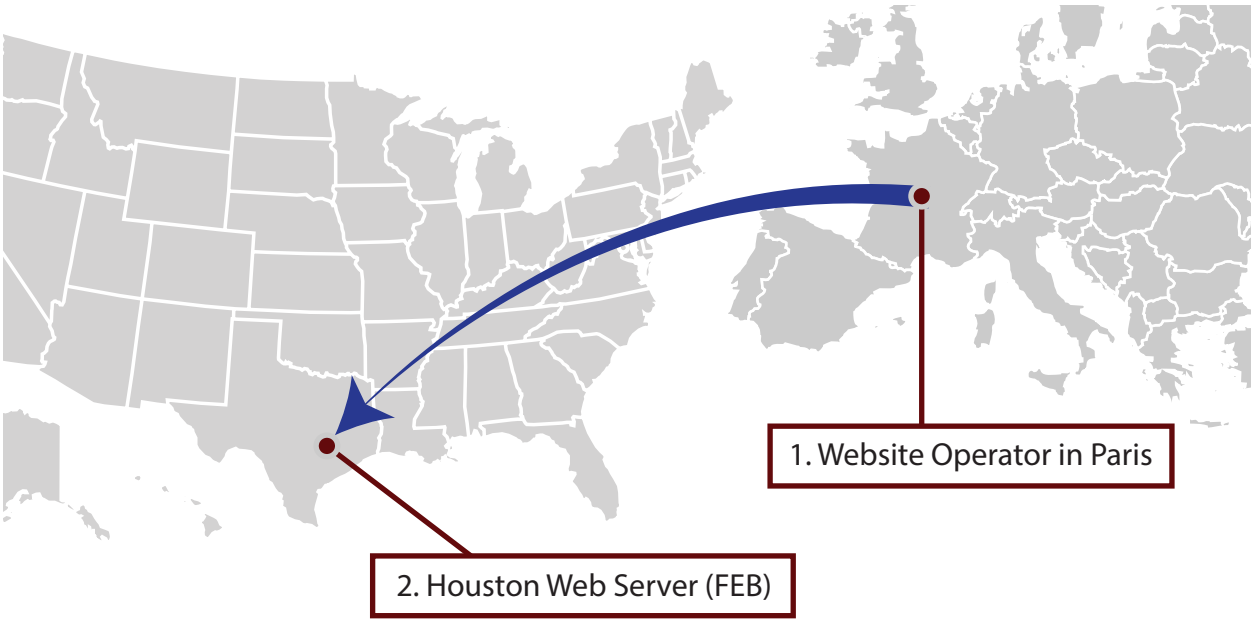
Functional Equivalents of the Border

The concept of the Functional Equivalent of the Border (FEB) is critical to border security because it allows the legal imposition of regulatory requirements (search, inspection, and seizure) away from the physical borders. In order to have an FEB, circumstances must exist which create the same environment as the border: those being: 1) there is a "nexus" to the border, a border crossing, or to something which has crossed the border; 2) there is a reasonable certainty that there has been no material change since the nexus with the border; and 3) the search and/or inspection occurs at the first practical detention point after the border crossing.[4] It is this same type of interpretation of the FEB that makes defining the cyber border largely possible.

The Cyber Border

The simplest method to define the cyber border is to apply the land border concept. The place where data transmission cables cross the physical national borders would constitute a border crossing. This analogy is deficient, however, since data can cross the border via other means independent of terrestrial data transmission cables – via satellite for example. It is also impractical for border protection and inspection for the same reason inspection of an in-bound aircraft at 35,000 feet is impractical. The cyber border therefore is best defined as the FEB where the data arrives at the first practical point of inspection— a network router, computer server, PC, or other networked device.

The web site example depicted in figure1 demonstrates the FEB concept applied to the cyber border. It depicts a World Wide Web (www) site involved in the sale of some type of illegal merchandise. This merchandise could be any item that would constitute an illegal import at the border such as controlled substances, counterfeit products, or child pornography. In this example the web site is hosted on a server located in the U.S., but directly managed and controlled by a foreign located criminal.

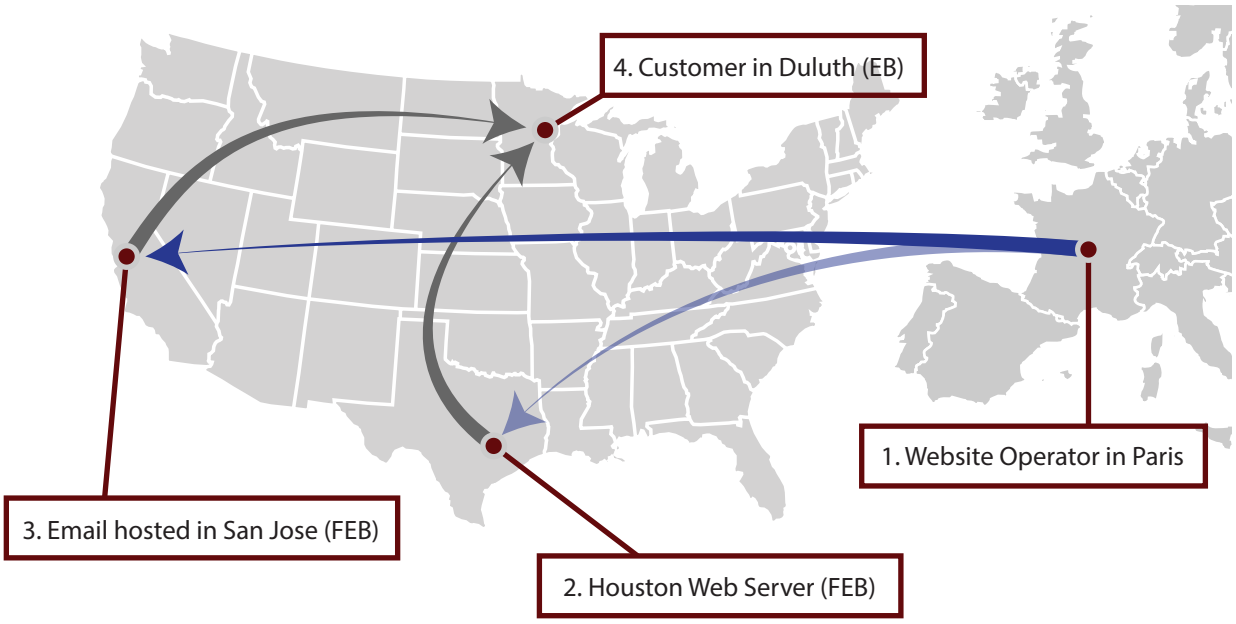


The website operator in Paris (1) logs into their web hosting account in Houston (2) and uploads merchandise (software, music, movies, etc.) that is advertised for sale and download from their web site. The Houston web server becomes a Functional Equivalent of the Border (FEB).

Figure 1. Example of direct delivery of merchandise from a foreign entity

The illicit web site in the example above could be providing information on the merchandise for sale, how to place an order, how to pay for the merchandise, and the options to arrange delivery. In the case of Internet deliverable merchandise, the web site can also be the point where customers access and retrieve (download) the merchandise; alternately the customers could also be directed to a second web site or file server to download the merchandise. Still another option is it that the customer can receive the merchandise directly as an email attachment from the seller from either a foreign or domestic email server.

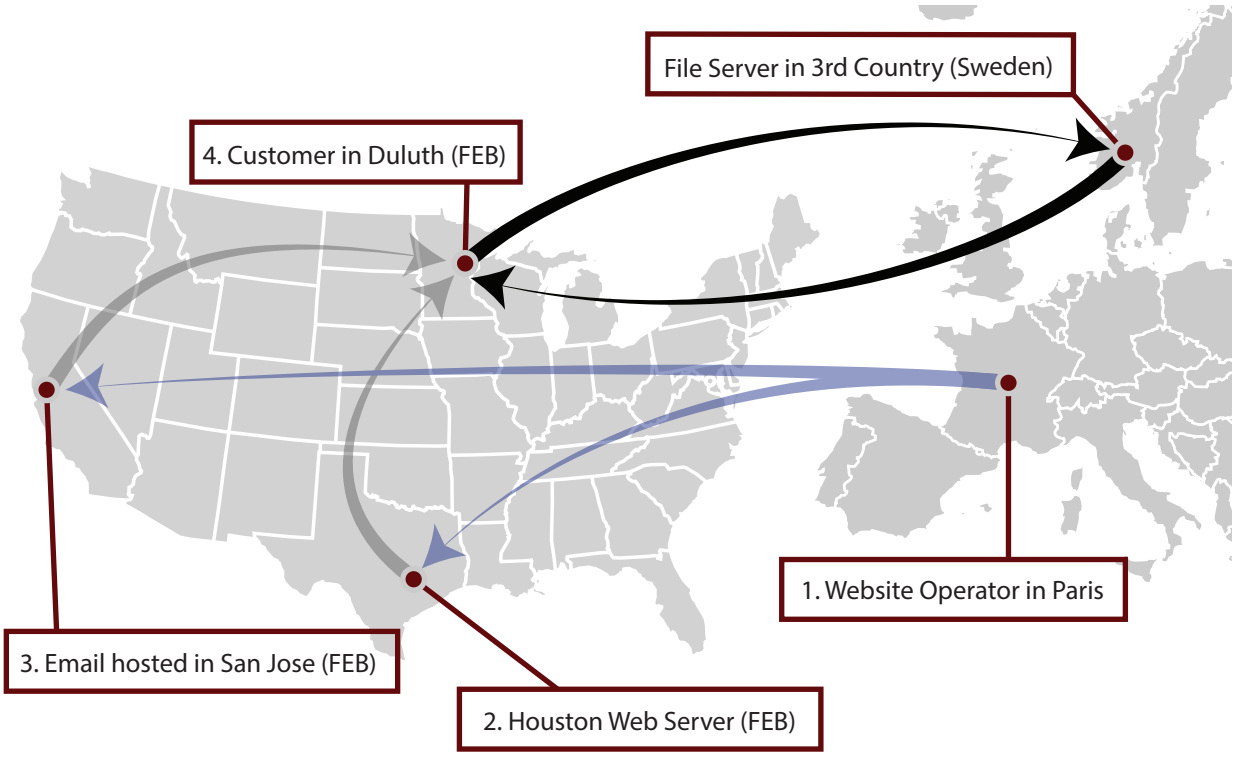
Figures 2 and 3 depict more complex scenarios for an illicit web site that involves the interpretation of multiple FEBs involved in the ordering and receipt of illegal imports.



3. The website operator in Paris receives customer orders and sends invoices and download instruction to customers via their email account hosted in San Jose which becomes a Functional Equivalent of the Border (FEB).

4. A customer in Duluth sends an order for merchandise via email to the seller's email account hosted in San Jose and receives the order invoice and the download instructions from the seller. The customer then downloads the merchandise from the seller's website in Houston directly to the customer's computer which becomes and Extended Border (EB).

Figure 2. Example of direct delivery of merchandise from a foreign entity with multiple FEBs



4. Customer accesses seller's file server in third country (in this example Sweden) and downloads the merchandise directly to their computer. The customer's computer effectively becomes a Functional Equivalent of the Border (FEB).

Figure 3. Another example of direct delivery of merchandise from a foreign entity with multiple FEBs

Critical to the understanding of how the FEB concept applies to defining the cyber border is an understanding of border enforcement authorities and how they work to protect the nation from border threats, while also addressing important constitutional and privacy concerns.

Border Search Authorities and Their Application to the Cyber Border

One of the most important border protection tools is the border search authority. This long-standing authority held by Customs officers and other authorized officials dates from the time of the nation's founding and is derived from some of the first statutes passed by Congress.[5] Based on Congress's broad authority to regulate foreign commerce and enforce immigrations laws, border search authority is a long- established exception to the Fourth Amendment's probable cause and search warrant requirements. [6]

The contemporary threat from terrorism and a basic interest in national self-protection make border search authority a necessary and legally accepted exception to normal 4th Amendment concerns. Border search authority allows for the warrant-less inbound and outbound search of persons, conveyances, and merchandise at the borders, the functional equivalent of the border, and in some other cases away from the border at what is referred to as the extended border.[7] While traditional border searches focus on the inspection of people, conveyances, and merchandise, the focus of cyber border searches would focus on the import and export of digital merchandise.

The primary purpose of a Customs border search is to inspect persons, baggage, and merchandise to ensure that duties are collected and to ensure that whatever is entering or leaving the country is in compliance with U.S. law.[8] Another important purpose of these searches is to search for and seize prohibited imported or exported merchandise. The definition of merchandise is "goods, wares, and chattels of every description."[9] If there is any debate as to whether the data carried over the Internet is merchandise it would come as a surprise to the thousands of copyright owners and vendors of software, music, movies, and books which are delivered to millions of customers daily via the Internet, or to the customers who pay for this digital merchandise. The debate on whether digital data is imported or exported in the traditional sense can be argued as being a function of the origin and ultimate arrival country of the digital merchandise. The illegal material or contraband which can be and is imported and exported via the Internet runs the gamut from child pornography, to counterfeit or illegally copied software and music, to stolen credit card information, to seditious materials— all materials which would be subject to seizure as imports or exports contrary to law.[10]

Of special importance to the cyber border discussion, particularly in the area of border inspection, is the inclusion of documents within the purview of a border search.[11] As stated previously, web sites advertising the sale of some type of merchandise can be simply that, an advertisement for a product, which provides a channel for the customer to contact and arrange the purchase and delivery of the merchandise. These contacts and arrangements can be accomplished through a variety of avenues including via email, web messages, or via an advertised telephone number on the web site. In the case of a web site being controlled by a foreign source, the email associated with the web page will likely contain information relating to the orders for these products and services and should be considered as documents relating to the importation of the merchandise. In the illustration examples, the emailed documents pertaining to orders from customers, whether those customers are located in the U.S. or elsewhere, are retrieved by the foreign source from a domestically located U.S. email or web server and transferred/exported to their foreign source's location. Conversely, documents relating to the orders sent from the foreign source to customers in the U.S. are sent from the foreign source's computer and are imported to their email server located in the U.S. In a traditional border search scenario, documents arriving from a foreign source, whether carried on a person, in baggage, or accompanying the merchandise, would be subject to search and examination to see if they pertained to the importation of goods. These same documents arriving via the Internet are not subject to this same search.

A domestically hosted but foreign-manipulated web site can not only serve as simply an advertising and ordering mechanism for merchandise that is shipped via traditional parcel service or mail, but can also serve as the actual delivery vehicle for the merchandise. Web sites that offer digital merchandise such as software, music, and videos commonly store the merchandise in separate file directories on the web host computers that the customers pay

to access. In such cases it is reasonable to assume that the digital merchandise placed in these file directories by the foreign source was imported to those computers by the foreign source from their foreign location. In most cases this can be verified by inspecting the IP history logs maintained by the web hosting company. The digital merchandise located on a domestic web hosting company computer/server that has been imported to that computer/server by a foreign web site operator should be subject to a Customs border search as an FEB.

Legal Merchandise versus Prohibited Merchandise

The Internet border search issue goes well beyond just the concern of illegal imports and contraband, but also to the much wider subject of general merchandise being imported via or assisted by the Internet. The exponential growth of Internet e-commerce represents legitimate commerce by both individual consumers and corporations. Internet border search authority may eventually be required to fulfill the other Customs missions of protecting the nation's revenues and for the proper assessment of duties. While the immediate impact that the addition of Internet/cyber border authorities would be most evident in the suppression of smuggling and other illegal activities, the benefit to the overall revenue protection may eventually prove just as significant.

Merchandise versus Communications

Current border search authority allows authorized officials to search for imported or exported merchandise including documents, at the border or its functional equivalent. This discussion of redefining the border for the purposes of enforcing a cyber border is not directed at private communications unless those communications pertain to an importation or exportation of merchandise— legal or otherwise.

Privacy Issues and Concerns

The cyber environment should not enjoy any enhanced protections over what persons should rightfully expect in the traditional physical world. Therefore, privacy issues involving the cyber border should be of no greater concern than in a traditional border situation. Since the focus of cyber border enforcement is on merchandise (legal and illegal, entering or exiting via the cyber border), private or privileged communications are already protected from inspection the same as in non-border situations.[12] Only data containing merchandise or documents relating the import/export of merchandise, legal and illegal, would be subject to inspection and border search and seizure. Granted, the cyber world does present some issues which may not have a corollary in the non-cyber world, but just as the evolved view of the traditional border must be adapted, so must the interpretation of border authorities so they may evolve to address the uniqueness of the cyber environment.

Conclusion

The importance of defending the nation against cyber threats is critical to national and homeland security. The magnitude of current and emerging cyber threats is equal to and may in actuality surpass traditional threats. The asymmetrical nature of cyber provides to minor nation-state enemies and even lone wolf actors the ability to inflict great harm to a great military power like the United States. Criminals do and will continue to exploit cyber to their advantage rendering many aspects of traditional crime prevention ineffective or obsolete. Stopping and preventing foreign threats at the border has been and always will be a key element in protecting the nation and its people. Adapting and evolving our definition of the border to define a national cyber border will help deny this pathway for foreign threats into our country.

About the Author

Mr. Phillip Osborn, Supervisory Special Agent (ret.), is a 35 year law enforcement veteran who has spent well over 2 decades conducting and leading computer and Internet related investigations and operations. Mr. Osborn has served as the chairman of the World Customs Organization Electronic Crimes Experts Group, and he has represented the U.S. Government as a subject matter expert on cyber related topics to numerous national and international organizations. Some of his work dating from the early 1990s provided the foundation and motivation for the establishment of U.S. Customs Cyber Crimes Center, as well as the creation of the Internet Crimes Against Children Task Forces. For over 7 years he served as the U.S. Customs/ICE National Program Manager for Cyber Crimes, leading operations, investigations, and policy initiatives to address homeland and national security threats. One particular initiative he championed was in the area of the convergence of traditional border security with the cyber domain. Mr. Osborn earned his graduate degree in homeland security studies from the Naval Postgraduate School, and has completed other graduate work in information security and in global strategic intelligence studies. Mr. Osborn's most recent assignments prior to retirement were leading a DHS border security and tactical intelligence initiative, and serving as the director of a joint DHS cybercrime task force. He may be reached at iamoz@comcast.net.

Notes

1 National Oceanographic and Atmospheric Administration- Office of Coast Survey, https://www.nauticalcharts.noaa.gov/staff/law_of_sea.html (accessed March 2. 2017).

2 Ibid.

3 Stephen R. Viña, "Protecting Our Perimeter: 'Border Searches' Under the Fourth Amendment," (Congressional Research Service The Library of Congress, August 2006), 7.

4 Ibid,7.

5 Ibid, 6.

6 Ibid, 6.

7 Ibid, 8.

8 See 19 CFR 162.6 - Search of persons, baggage, and merchandise.

9 See 19 CFR 146.1 - Definitions

10 Ibid.

11 US Customs and Border Protection Policy Regarding Border Search of Information, https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf, *(accessed March 2, 2017).*

12 Ibid, 4.