*THE U.S. CAN HELP AFRICA
SOLVE ITS OWN REGIONAL
SECURITY PROBLEMS BY
CONTINUING TO DEVELOP
A BROAD, LONG-TERM
COOPERATIVE SECURITY
RELATIONSHIP WITH AFRICA*

to positioning a USAFRICOM headquarters in Africa.⁴⁹ It would also address regional security issues more effectively by leveraging expertise at the U.S. State Department, think tanks and other Washington-based intellectual resources, such as the United States Institute of Peace and the U.S. Department of Defense Africa Center for Strategic Studies. Consolidating these options and other policy initiatives into an all-inclusive package would strengthen U.S. Africa policy and strategy formulation and could be a useful template going forward.

CONCLUSION

The U.S. has been able to pursue a policy of fostering regional security and stability in Africa, including support for African-led solutions to regional security issues, by using USAFRICOM as a mechanism for policy implementation. Unquestionably, the U.S. can help Africa solve its own regional security problems by continuing to develop a broad, long-term cooperative security relationship with Africa, including the use of USAFRICOM as a regional framework for U.S. security cooperation with African states and regional organizations. The U.S. certainly has a stake in preserving and strengthening the international state system, including Africa, especially given its global leadership position. Such strategic cooperation should also dispel the myth regarding the possible militarization of U.S.

policy toward Africa.

U.S. policy toward Africa can be seen in U.S. policy documents, such as the U.S. National Security Strategy, Quadrennial Defense Review, U.S. Strategy toward Sub-Saharan Africa, and other strategic guidance. The role of USAFRICOM in regional security issues in Africa can also be readily derived from such documents. U.S. policy toward Africa crafted in Washington has been instrumental in shaping USAFRICOM, including its purpose, regional plans and strategies, command structures, regionally-tailored forces and forward operating locations. Clearly, USAFRICOM has played a stabilizing role in the region, and changed perceptions to some degree by articulating its purpose to regional stakeholders, soliciting feedback, and aligning itself with U.S. Africa policy and objectives. Undoubtedly, USAFRICOM has helped build the security capacity of African states and regional organizations, especially for regional peacekeeping, and humanitarian and disaster relief. The continued success of U.S. policy toward Africa will depend on its applicability and credibility, including the appropriate use of USAFRICOM for policy implementation. It will also depend on USAFRICOM's ability to help shape U.S. policy toward Africa based on its cumulative experience in the region – and refining the rough edges of a regional strategy within which any U.S. regional command will inevitably be viewed.

AN ANALYSIS ON THE
REGULATION OF GREY
MARKET CYBER MATERIALS

KELSEY ANNU-ESSUMAN
Yale University

EXECUTIVE SUMMARY

This paper analyzes the grey market for cyber materials by evaluating the current nature of transactions within the market. This paper claims that vendors ought to be required to disclose information (to companies) on the vulnerabilities, exploits, and botnets that are sold. Analyses include:

a) Historical cases of weaponized cyber materials

b) Statistics on the costs associated with the grey market

c) Explanation of risks associated with unregulated grey market activity

Limitations to mandatory disclosure outlined in the paper include the:

a) Culture of anonymity within the market

b) Appeal of lucrative job prospects for hackers who rely on the secretiveness of the market

c) Perception of risks

Another overarching, key argument presented for non-regulation is the need for government agencies to preserve their access to tools of offensive warfare that are bought on the grey market.

In response to limitations, this paper finds that mandatory disclosure would, at minimum, allow software companies the opportunity to further pursue the protection of their systems and limit the risks of an unregulated

market. This paper finds that enabling software companies best serves the interest of overall security and does not completely undermine the ability for government agencies to purchase offensive mechanisms.

INTRODUCTION

The creation of the computer network system and its spread throughout the international realm has opened doors for new ways of gathering information as well as manipulating this information for both protective and malicious purposes. While the material stored within computer systems is often thought of as being privy to the user of that system and whomever the user decides to share their data with, the rise in cyber-attacks has proven otherwise. Cyber “crime” or “attacks”—the exploitation of Internet and, more generally, computer vulnerabilities in order to access and use private information—rose as personal data began being stored on system networks since the nascent years of the internet.¹ Policies such as the Computer Fraud and Abuse Act of 1986² and the proposed National Defense Authorization Act for 2014³ have establish(ed) guidelines for unauthorized tapping into the systems of the U.S. government as well as financial and commerce institutions. While cyber-attacks were initially thought of as a method used by individual or small bands of hackers attempting to access information for

WITH THE ONSET OF
LARGE-SCALE CYBER
ATTACKS, IT HAS BECOME
CLEAR THAT THE TITLE
OF “HACKER” IS NO
LONGER RESERVED FOR
INDIVIDUALS BUT EXTENDS
TO GOVERNMENTS AS WELL

THE MONETARY INCENTIVE FOR HACKERS TO SELL CYBER MATERIALS AND INFORMATION IS RELATED TO THE CHANGING NATURE OF THE CYBER REALM

personal use⁴, discussions of cyber-crime have shifted to the offensive mechanisms of hacking employed by governmental organizations. With large-scale attacks such as the Morris worm replicated in UNIX systems across the globe in 1988⁵ and, more recently, the infection of 30,000 Saudi Aramco (world’s largest oil producer) networks with a self-replicating Shamoon virus in 2012,⁶ it has become clear that the title of “hacker” is no longer reserved for individuals but extends to governments as well.

The rise in government probes into both domestic and foreign security systems reveals that while there is a significant amount of information to be gathered for important national security purposes, there is also a significant level of risk in the methodology of information gathering.⁷ Risks are exacerbated by the types of markets available for purchasing exploits and botnets or merely the information on system vulnerabilities that can be crafted into an exploit. The three forms of markets – the white market, grey market, and black market – all pose significant dangers in that they compromise the information of buyers, purchasers, and those who will be affected by the use of the cyber material being sold. This paper focuses on the clandestine and unregulated grey market where government authorities, defense organizations, and other pseudo-political groups are able to purchase their cyber material. Given the market’s secrecy, this paper argues that regulatory measures ought to be imposed on

grey market transactions. More specifically, vendors should be required to disclose the vulnerabilities and exploits to computer software companies (in this essay, synonymous with the term “manufacturers”) prior to making the information marketable to purchasers. Provisions for providing this information ought to be mandatory in an effort to ensure that companies have been given ample ability to secure their data and the data of their users. This suggestion is based on the notion that defensive measures of securing information ought to be prioritized over the potential to create offensive attacks using holes, or “vulnerabilities,” in security.

I begin by outlining the general functions of the grey market. Here, I explain the uses of the cyber materials—namely for offensive security tactics by government authorities and defense contractors. In describing the buyer-seller dynamic, I outline the effects of anonymity and monetary incentives on vendors within the market. I remark on the limitation these dynamics place on regulation. Following this, I explore the possibility of regulation through a previously advocated technique, professionalization, and the mandatory disclosure. In exploring regulation, I discuss the types weapons sold in the market and types of buyers. I narrow my analysis to the type of cyber-material predominately bought and sold in the market: zero-day exploits. My explanation of zero-day exploits includes the

risks associated with cyber materials being indiscriminately made available to all types of actors. Throughout my analysis, I consider concerns of feasibility. In discussing the merits of market regulation, I hope to demonstrate that regulation is essential to ensuring security for the systems vulnerabilities infect.

THE GREY MARKET ALLURE

A description of the grey market yields three features key to its function as an unregulated space: the culture of anonymity, the potential for large monetary gains, and (most relevant to government and defense agencies) the potential for gaining information necessary for offensive attacks. Anonymity—the confidentiality of actors and specific materials on the grey market—is a particularly important issue to both sellers, and most especially buyers. Understandably, agencies prefer to keep their purchases unknown to the general public, as their activity within the grey markets is part of national security intelligence and defense informational tactics.⁸ For example, the Grugq—an exploit broker—faced immense pressure and backlash in the form of decreased demand for his informational products after exposing in an interview⁹ the payments and customers he receives for cyber exploits. The nature of the market means that the threat of backlash and subsequently lost revenue undermines efforts to expose information and reinforces

the culture of anonymity. Secondly, individual hackers who discover system holes—be it at hacking conferences amongst colleagues and potential buyers or within the privacy of their home—can make upwards of 15% from their sales.¹⁰ The monetary incentive for hackers to sell cyber materials and information is related to the changing nature of the cyber realm. Perlroth and Sanger note, “Ten years ago, hackers would hand knowledge of such flaws to Microsoft and Google free, in exchange for a T-shirt or perhaps for an honorable mention on a company’s Web site”.¹¹ As cyber security is becoming more and more part of the U.S.’s national security discourse¹², authorities are seeking assistance from those with intimate knowledge of the hacking community. As a result of the changing face of cyber attacks, hackers are now being sought out by reputable states agencies such as the National Security Agency¹³ who have become “open advocates [of the hacker community], willing to buy technology, and fund research”,¹⁴ as their work is being demanded by the shifting nature of warfare and the intelligence agency. Initially, infiltrating the hacker community had its own challenges, particularly in the area of trustworthiness amongst hackers and governments. To mollify suspicions, transactions were based on a level of anonymity. This was necessary for hackers who had previously been targeted by government agencies and for governments who did not yet have the intelligence and expertise

CURRENTLY, INDIVIDUALS WHO WERE ONCE STIGMATIZED AS CRIMINALS ARE PARTS OF A LUCRATIVE MARKET THAT REINFORCES THE SPECIFICITY OF THEIR WORK

to verify information retrieved from hacking communities. Currently, individuals who were once stigmatized as criminals are parts of a lucrative market that reinforces the specificity of their work. This also means agencies are willing to pay more in order to remain atop of the demands of the shifting cyber tools, thereby reinforcing the effects of anonymity and monetary incentives.

While supply and demand in competitive markets would predict that the lucrative market for hackers would create an opposing market for researchers seeking to patch loopholes, this is not currently the case. Despite the work that some researchers do to uncover vulnerabilities and forewarning software companies of future breaches, these individuals are oftentimes not compensated for their work—even by large corporations such as Adobe and Apple¹⁵. In fact, independent hackers who sell their findings to grey market vendors make close to “10 or even 100 times” more than what researchers can receive for providing information to companies such as Facebook and Microsoft¹⁶, thereby creating an indisputable disincentive to assist companies. Efforts such as the “Hacker One” initiative by Facebook and Microsoft as well as the Texas-based Zero Day Initiative¹⁷ have attempted to amend the problems of compensation for disclosure by paying researchers \$300 to \$5,000¹⁸ for their knowledge of any malware, vulnerabilities, or exploits that will later be sold. On Hacker

One, discussions of vulnerabilities or “bugs” are made open on feeds that also list who have earned certain compensations or “bounties” for their contributions.¹⁹ Hackers can even ban together forming “teams” for exploring holes in systems and reporting back to Hacker One.²⁰ Yet, it is clear that any effort to require disclosure by hackers to companies would have to offer comparable monetary incentives to promote cooperation and avoid the risk of merely driving transactions even further underground into deeper spaces of anonymity such as the black market for cyber materials. Hence, international regulation within the hacker and cyber researcher communities is limited.

MANDATORY DISCLOSURE AS REGULATION: A POSSIBILITY?

Within the grey market is a culture of indiscriminate transactional practices, which pose difficulties for requiring disclosure, beyond concerns of monetary incentives. Buyers and sellers that are not held accountable by outside standards are susceptible to equipping organizations with malicious intent with the products they need to carry out their actions. One suggestion to rectify this risk is to make the grey market sellers “official” by professionalizing their practices. Although this suggestion is more focused on changing the perception or connotation associated with the clandestine sale of cyber materials, professionalization would

AS A RESULT OF THE CHANGING FACE OF CYBER ATTACKS, HACKERS ARE NOW BEING SOUGHT OUT BY REPUTABLE STATES AGENCIES SUCH AS THE NATIONAL SECURITY AGENCY

involve setting normalized standards for the industry. The goal of professionalization would be to “regulate workers...enhance public trust...and enable compliance with regulatory requirement” among other goals.²¹ Presumably, this would involve standardizing requirements on the levels of schooling needed to enter the cyber security field, assessment of skills related to the industry and general career preparation/etiquette when handling personable, vulnerable information. Not only would standardizing the players of the market entail requirements for credentials such as certifications for hackers and required training for properly handling sensitive information, but it would also affect the way vendors presently operate by not screening their buyers. The well-known French organization Vupen, which specializes in identifying vulnerabilities to be sold for large sums (sometimes \$1 million),²² refuse to reveal their clientele.²³ By not screening buyers, Vupen and companies like it create the potential for maliciously intended agencies to gain access to their vulnerabilities without any pushback from regulatory practices.

Professionalization seems to be a more attractive option to naturally regulate grey markets because it involves altering the culture of the market. Yet, determining hiring practices, specifying types of skill sets, and giving guidelines for the type of education necessary to enter into these markets as a vendor or identifier of vulnerability are difficult tasks. In

this way, the capricious and blanketed nature of discovering vulnerabilities and creating exploits hinders professionalization. Hence, what works in one instance of uncovering and creating a potential exploit to be sold may not be sufficient or necessary to effectively identify holes in another scenario. The consistency of professionalized standards is, in fact inconsistent with the market itself.

Another suggestion, the one advocated in this paper, is to make transactions a liability for the seller.²⁴ If the seller is required to demonstrate proof (either via documentation or exchanges between the vendor and company) that the vulnerabilities and exploits being sold have also been given to the manufactures of the systems that the holes are within, then the risk of those vulnerabilities being given to anonymous buyers is mitigated, if not eliminated. The most salient issue surrounding anonymity, as mentioned before, is that the intention of the buyer is unknown. In the case where a company has been made aware that their systems could be compromised, the company could now be held liable for breaches and have the responsibility of pursuing measures to mend the breach. Intentions of buyers are then made irrelevant, since, regardless of who knows the vulnerability, the company is well informed on how to protect themselves and their users.

While the approach of liability is most beneficial in cases where the intentions are unclear, the viability of requiring disclosure of

THE UNITED STATES AND ISRAEL WERE LATER REVEALED AS BEING THE INITIATORS OF THE CYBER-ATTACK, WITH 60,000 COMPUTERS IN VARIOUS COUNTRIES AROUND THE WORLD

information from sellers of vulnerabilities is complicated by situations where the vulnerabilities can be used for preventative (offensive) purposes. Perhaps the most salient issue related to feasibility is the need to preserve avenues for cyber information gathering to be used in offensive activities. Government and defense agencies typically purchase cyber materials as tools for espionage and claim these practices as legitimate forms of warfare and, more benignly, national security. The offensive nature of espionage relies on the fact that the exploit is used to obtain information to help promote other security initiatives. Claims to the necessity of offensive attacks are difficult to counteract since the idea of offensive tools is not foreign to the realm of warfare. The case of Stuxnet illuminates a concern in providing governments with access to vulnerabilities on a private marketplace. Stuxnet, a zero-day weaponized computer program discovered in June 2010 by VirusBlokAda, was developed from codes exposing vulnerabilities in Windows systems.²⁵ The United States and Israel were later revealed as being the initiators of the cyber-attack, with 60,000 computers²⁶ in various countries such as the United Kingdom, Germany, South Korea, China, and India being infected and over 60% of the worm infections taking place in Iran.²⁷ The sheer scale and global nature of the attack was not the sole reason for concern. Stuxnet disrupted the frequencies within centrifuges of Iran's nuclear facilities,

thereby becoming the "first industrial-sized" attack using malware. The intention was to isolate systems within Iran; however, the fact that 40% of the worm was replicated in other nations exposed risks related to collateral damage.

The concern, related to the idea of intentionality and anonymity, is that two subsets of users of the grey market—terrorist organizations and "rogue" governments – may have (or already do have) the same information as more favorable (or trustworthy) buyers. Furthermore, regulation, as during prohibition, can cause otherwise visibly detrimental actions to become less visible and transactions to occur in the "underground" black market. Having exploits and vulnerabilities in that market is potentially even more risky since knowledge of where these markets are and who is partaking in transactions is kept secretive, in addition to what is being sold. And, even more starkly different from the grey market, black-market cyber materials (oftentimes counterfeit)²⁸ are sold at cheap prices to attract purchasers who would be more inclined to buy from more secure vendors at the same price. Furthermore, materials are oftentimes counterfeit.

THE TRAJECTORY OF CYBER WARFARE AND PERCEPTION OF RISKS

Thus far, the focus of this paper has been on the actors of the grey market and the

THE QUESTION OF THE NECESSITY OF REGULATION CANNOT FOCUS SOLELY ON CONCERNS OF WHO IS SELLING AND WHO IS PURCHASING

risks associated with their participation. The question of the necessity of regulation cannot focus solely on concerns of who is selling and who is purchasing. Rather, there is also a question to be considered about what is being sold; and the main product on the line is one that has been linked to growing discussions on the future of cyber warfare: exploits. Zero-day exploits are known as the most detrimental compromises of software because they are classified as "unknown threats". Thereby, zero-days cannot be mended by anti-spyware or malware protections already in place within a system.²⁹ Sold on the "high-end" level of the grey market at "up to \$250,000,"³⁰ once a zero-day has infiltrated a system, the effects are immediate and system managers do not have time ("zero days") to reverse and patch the holes within the system.³¹ Zero-days are considered to be "weaponized" once they are used "to disrupt, disable, or destroy computer networks and their components."³² While zero-days are the most prevalent types of exploits to be weaponized, the information needed to transform a system into a botnet can also be found in the grey market. Specifically, a botnet is when hackers use malware to control systems remotely, thereby being able to access private documents and information stored on systems, as well as control commands with the computer(s).³³ These controls can be used for espionage or fraudulent purposes.

Cyber war has become more of

a catch phrase because of the prevalence of interconnected informational and communications technologies; yet, the perception of risk is a limiting factor in how willing individuals are or will be to abide by disclosure requirements. Currently, many still believe that cyber war is not imminent and that the manipulation of systems technology is confined to the realm of personal theft, such as identity thieves or clandestine government activity that ought to remain privy to the Department of Defense and National Security Association. Yet, the real concern surrounding cyber materials purchased in the grey market by ill-intended actors lies in the ability for information and communications technologies now to be used for targeting "electrical grids, food distribution systems, [and] any essential infrastructure that runs on computers."³⁴ Perceptions of risk matter in so far as hackers are individual members of these communities. They are also the ones who can create a culture within the hacking industry of either ambivalence towards the growing potential to cause physical damage or activism for safer methods of utilizing information for the sake of all those involved.

Companies who sell informational and technological material face enormous costs once their information is compromised. The International Criminal Police Organization (INTERPOL) acknowledges these large costs in their 2007 and 2008 estimates of sums paid to retroactively rectify attacks against gaps in soft-

ware. INTERPOL notes, “The cost of cybercrime worldwide was estimated at approximately USD 8 billion. As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth up to USD 1 trillion” — larger than the budget of INTERPOL itself.³⁵ Similarly, Intel reports that the “US government alone spent \$25 million purchasing code vulnerabilities”³⁶ making it the largest spender on material for potentially offensive exploits in comparison to states such as Russia, China, and North Korea. While the U.S. government justifies their purchases through claims of using information for offensive attacks, it is unclear whether the same discretion can be trusted in the hands of other actors within the grey market, as mentioned above. Terrorist organizations are also able to purchase exploits and vulnerabilities, and the absence of external checks on their purchases means that they are unregulated in the most extreme sense and have the ability to weaponize vulnerabilities. Essentially, mandatory disclosure has the potential to minimize these costs by creating a safety net for software companies who have the human capital to invest in finding solutions to patch the holes in their software, but do not necessarily have information on where these holes are located.

CONCLUSION

At the beginning of this paper, I hoped to demonstrate the necessity for regulating the grey market of cyber materials. The value in regulating the grey market was based in the idea that informational security ought to be prioritized over offensive security measures that could be pursued by access to system vulnerabilities. Throughout this paper, it has become clear that these two intentions — securing information and pursuing offensive attacks — are not mutually exclusive. With cases such as Stuxnet, government agencies have used the vulnerabilities and zero-day exploits purchased from grey market vendors as a means of preventative action. Yet, the feasibility of requiring sellers to disclose information of their “products” is limited by the attractiveness of lucrative jobs in hacking as well as the

willingness of buyers and sellers in the grey market to impose regulations on their practices, as demonstrated by the stance of organizations like Vupen. Despite these limitations, it is necessary to consider mandatory disclosure as an option because of the real risks associated with maintaining a secretive market for cyber materials. These risks are amplified by the types of materials primarily sold in the grey market (zero-day exploits) and the types of buyers attracted to the market’s clandestine nature (organizations with potentially malicious intent). While government agencies argue the necessity of the grey market for purchasing offensive warfare material, the necessity to protect individuals ought to be valued over protecting an interest in maintaining a wide array of national security tools. Requiring the disclosure of vulnerabilities would enable companies to pursue security measures while not fully hindering buyers from purchase exploits and vulnerabilities on the grey market.

ICELAND’S CLEAN ENERGY ECONOMY

A ROADMAP TO SUSTAINABILITY AND GOOD BUSINESS

ÓLAFUR RAGNAR GRÍMSSON
PRESIDENT OF ICELAND

President Grimsson studied economics and political science at the University of Manchester, and in 1970, became the first person in Iceland to earn a PhD in political science. In 1973, he became a Professor of Political Science at the University of Iceland. He was the University of Iceland’s first Political Science professor. He served as a Member of Althing (Iceland’s Parliament) from 1978 to 1983. He served as the Chairman of the People’s Alliance executive committee from 1983 to 1987. From 1987 to 1995, he was Leader of the People’s Alliance; during this time, he served as Minister of Finance from 1988 to 1991 and as a Member of Althing from 1991 to 1996. He assumed office in 1996, ran unopposed in 2000, was re-elected in 2004, ran unopposed in 2008, and was elected for a record fifth term in 2012. In 2013, he announced the formation of the Arctic Circle, an organization designed for the facilitation of dialogue among political and business leaders, environmental experts, scientists, indigenous representatives, and other international stakeholders to address issues facing the Arctic as a result of climate change and melting sea ice. He is Iceland’s fifth President. He received an award for Iceland’s sustainable energy and economic policies in his tour of Cornell. The following is an edited transcript of his lecture.

I am deeply honored to be here today and to speak about a matter which is very dear to my heart but which is also of fundamental importance to the future of our planet. But, let me first also recognize, as you mentioned this morning, when I paid my homage and expressed the gratitude from the people of Iceland to Cornell and to the people of your library for preserving here at the university the greatest collection of Icelandic books, old and new, some of them more than 500 years old, to be found anywhere outside of Iceland, and for more than 100 years this great university has preserved this collection and renewed it every year, and thus becomes the center of study and research and awareness on the great literary heritage of my country. This is not just of significance to Iceland, but the sagas written in Iceland in the 12th and 13th century when the rest of Europe used Latin, are indeed to western literature as temples and ruins and Athens and Rome are also to western civilization. So why this great university preserve this collection and uses it as a forum for research and discussion, you are not just honoring my own country, you are also preserving one of the most important legacies and pillars of the western civilizations. Let me again here today in this public hall thank the university for this extraordinary contribution and all the people alive and those who have passed away for having dedicated their lives for preserving the physical collection here at the

university.

So in a way it is both an honor and a privilege and also a reminder of our responsibilities that I come here today also to talk about the future of our shared planet not just to pay homage to what was done in my country eight or nine hundred years ago, but also to enter

PRESIDENT GRÍMSSON