Blind Spots and Counterfeits in the Supply Chain

Lessons from Haiti that can be well applied to the Philippines and Hawaii

Alison Kuzmickas, Steve Chan, Robert Spousta III, Simone Sala
Dr. Steve Chan Center for Sensemaking, AIRS
Swansea University NSRC and Hawaii Pacific University
Swansea, Wales, U.K.; Honolulu, HI, USA
Email: akuzmic@mit.edu, stevechan@post.harvard.edu, spousta@mit.edu, salas@mit.edu

Abstract—**Collaborative Big Data Analytics involve a variety of techniques for information gathering and source authentication, including crowdsourcing data. In turn, the development of crowdsourced and participatory mechanisms for a more transparent supply chain is pivotal to identify blind spots and mitigate their impact on global citizens' health and safety. Such effort is also instrumental in reducing cyber risks from the digital world that currently represent a major threat to the stability of national and international economic systems. The paper reviews the lessons learned from the earthquake that devastated Haiti in 2010, whereby the successful combined application of crowdsourced crisis mapping with standard disaster relief operations was equalized by the challenges of data verification for the authenticity of humanitarian products. By overviewing the threats to supply chains coming from the digital world, the paper proposes the adoption of next-generation network science tools to enhance transparency of global supply chains and reduction of cyber risks on the global society.**

Keywords-Big Data, Cyber-Physical Supply Chain, Decision Engineering, Social Complexity Science, Technological Innovation

I. INTRODUCTION

At first glance, the Haiti Earthquake and Tsunami of 2010 demonstrates the extraordinary value of modern day geolocative technological responses. Ushahidi, a geospatial platform that became the go-to for a number of 2010 extreme-scale disasters (including the January 12th and February 27th earthquakes in Haiti and Chile, respectively) propelled two ideas onto a global stage. First, it demonstrated the merit of Gartner Research Vice President Anthony Bradley's 2008 blog post that proclaimed "Every Twitterer as a Sensor" for the reporting of timely information, via Twitter posts and Short Message Service (SMS) text messages from disaster areas, so as to assist boots-on-the-ground officials in locating and prioritizing those victims with the most time-sensitive needs as well as to effectuate the point-of-need delivering of humanitarian and medical relief more rapidly. Second, it formulated the intersection graph for Kevin Ashton and the Massachusetts Institute of Technology Auto-ID Lab's ubiquitous computing mantra of the "Internet of Things" with Graham Cluley's descriptor of the current state of the Web — the World Where Web — in which everything is increasingly being tagged, tracked, mapped, and construed as part of a global supply chain.

With this study space clearly illuminated, we began to get a handle on the incredibly complex Wurlitzer of supply chain logistics that runs the gamut from inbound helicopters precisely choreographed with the whistling of extending flaps by landing aircraft, at the U.S. Air Force-operated Toussain Ouverture International Airport in Port-au-Prince (P-au-P), to the orchestral grinding of gears amidst the convoy of United Nations (U.N.) vehicles and the sharp metallic sounds of the local Haitian trucks, which serve as supply transports from P-au-P to the abutting rural areas of need in Carrefour, Leogane, Delmas, and Jacmel. However, just as the U.N. was about to plant the pennant of victory so as to memorialize its successful distribution of essential drugs and medical treatments to throngs of grateful Haitians, a locally well-known, but little advertised phenomenon (and **blind spot**) arose from an obscured subterranean position to a prominent surface location, and the ensuing tectonic shift sent a high magnitude shock wave through the entire humanitarian world; many of the crates chock-full of emergency supplies and medicines were filled with counterfeit pharmaceuticals [1].

In this paper, we explore vulnerabilities in the global cyber-physical supply chain, and offer mitigation strategies. In Section II, we begin by establishing the danger of counterfeit goods in the global supply chain through various recent examples. In Section III, we discuss the economic impact of counterfeiting on corporate brand images, and the need for increased private sector focus on cyber risk mitigation. In Section IV, we offer the "See Something, Say Something" mantra of citizen vigilance and homeland security as a means for enhancing resilience in the cyber-physical supply chain. In Section V, we discuss how increased transparency, when coupled with citizen vigilance and technological innovation can yield more resilient global supply chains, and we conclude in Section VI.

II. COUNTERFEITS IN THE SUPPLY CHAIN

Whereas having a fake Louis Vuitton bag does not pose any personal risk per se, counterfeit drugs pose a clear and present danger to both the patient and the provider of medical materiel [2]. In one stroke, the integrity of the savior white knight's supply chain was called into question, and as we obtained an increasingly deeper understanding of the P-au-P supply chain and engaged in a hermeneutic examination of the actual machinations for the supplying of

ISBN: 978-1-61208-423-7

the much needed humanitarian aid from the concerned-community-at-large to Haiti's devastated regions, our sense of organizational triumph was swiftly punctured. We quickly discovered that even with our dedicated and sustained efforts towards this worldwide-attention-receiving mission, our incredible preponderance of logistical force conjoined with the aggregate of multinational "no-expenses-spared" herculean technological muscle, with plenty of technological safeguards, simply was not sufficient to prevent the fact that large supplies of medicinal drugs in Haiti, in many instances delivered under the haloed imprimatur of a respected non-governmental organization (NGO) or sanctioned sovereign force, still turned out to be false and potentially harmful to those disaster victims, who desperately needed these supplies.

Even though P-au-P is no stranger to counterfeits (such as when it happily received from New York City, in April 2010, approximately $10 million worth of NYPD-seized knockoff footwear and clothing [3], which sported spurious labels ranging from Nike to Ralph Lauren), P-au-P also retains painful lingering memories of the death of eighty nine of its children who died from bogus cough syrup containing antifreeze [4]. The ever-increasing prevalence of these reported horrific incidents involving harmful counterfeit medicines is frightening: anti-inflammatories that contain leaded road paint [5], antibiotics that are made of talcum powder [6] or flour [7], and other purported life-saving pharmaceuticals that contain atrocious ingredients such as floor polish [8], sawdust [9], and rat poison [10].

The cry, "The evil of [fraudulent] fake drugs is worse than the combined scourge of malaria, HIV/AIDS, armed robbery, and illicit drugs" [11] echoes throughout the developing world, and some experts have estimated that there are about a million deaths a year from the consumption of counterfeit drugs [12]. Even in the cases for which there actually are some active ingredients in the sham drugs, the trace amounts are not sufficient to function effectively and, ironically, actually induce the virus (because there is insufficient potency to kill it) to mutate into an entirely new strain, thereby causing the unwitting patient to develop an irreversible resistance against subsequent treatments by legitimate medicines. It turns out that these pestilent counterfeits not only irreparably harm these innocent patients, but the fraudulent mislabeling and ensuing breach of trust for the alleged brand also tarnishes the reputation of the victim company.

Despite valid mitigating factors in each of these counterfeiting cases, the stigma and intensely negative perception attached to the incidents cannot be displaced or dispelled by the victim companies. The counterfeiting state of affairs has become a force onto itself, and the World Health Organization (WHO) has estimated that up to 10% of the world's pharmaceutical market is now comprised of these spurious drugs [13], and for some cases in Africa, Latin America, and Asia (including the Philippines), these counterfeits congest up to 30% of those markets [14].

The counterfeit pharmaceutical market equates to approximately U.S. $75 billion [15], and pharmaceutical firms must now diligently maintain global intelligence efforts and actively collaborate with law enforcement to search out, seize, and destroy counterfeit products in order to protect the integrity and reputation of their brands. From the myriad of various jurisdictions from around the world, the dedicated and indefatigable anti-counterfeiting hounds of law are more than eager to assist in these mutually reinforcing Public-Private Partnership Initiatives (P3I) because the involved host nation's economic success and progress is predicated upon the notion of uninterrupted trade; any lack of confidence in iconic brand names most definitely constitutes a barrier to the flow of goods.

Many iconic brand names have suffered, and the traditional top-down supply chain approaches are fraught with issues of opacity, particularly when corporate annual reports only necessitate peering at the primary layer of suppliers. In essence, operations ranging from the U.N. operations in P-au-P to large distributors and manufacturers, such as Wal-Mart and Boeing, amidst the increasingly convoluted supply chain web in these hard economic times, can no longer readily identify who the suppliers of their suppliers are. Traditionally, transparency is divided along two dimensions. Given a more constrained product line, and particularly if there is an extremely popular product, firms might provide complete transparency about just that specific product. In contrast, given an enormous product line or a wide swathe of involved components, transparency might only go one or two levels deep. When transparency does not run deep, there are blind spots and things can go bump in the night, for the nation as a whole, such as when a large company like Boeing is impacted.

In the case of the U.S.-based Boeing Company, it not only has an iconic brand, but it is also one of several large companies whose success or failure can have an enormous impact on the U.S. economy; an interruption of just a few weeks in the company's production contributed to a 6.2% decline in the U.S. Gross Domestic Product (GDP) in the fourth quarter of 2008 [16]. This recital of national factual significance underscores a core tenet and forms the touchstone for not only the treatment of counterfeits and the explorations for a crowdsourced participatory mechanism for a more transparent supply chain, but also for the revealing of an unexpected opportunity to simultaneously tackle another ominous national priority — **cyber risks in the digital world**.

III. COUNTERFEITS, CORPORATE REPUTATION, AND THE NEED TO BETTER MANAGE CYBER RISK

Given today's litigious climate, organizations across the board now take **cyber risks** very seriously, and nothing is more valuable to a business than its reputation [17]. Hence, cyber brand attacks, which leverage a company's valuable brand for nefarious purposes, are particularly dangerous. Firms, such as Novartis, assert that their brand depends upon their ability to assure patients that products bearing the Novartis label are, in fact, Novartis products, which are inherently underpinned by elevated unwavering standards of “quality, safety, and efficacy” [18].

The most vicious of cyber brand attacks is malware (malicious software) [19], and 38% of all cyber attacks use malware [20]; in fact, there are 60,000 new pieces of malware identified per day [21]. At a broad level, malware is best identified by us as simply the Google warning, “this web site may be harmful to your computer.” Behind the scenes, malware is designed to target the contact list of the victim of attack. The contacts might start receiving Viagra spam (unsolicited e-mail containing, in many cases, a payload such as malware) and other unsolicited email messages pertaining to a variety of pharmaceutical drugs. According to the *Verizon Data Breach Investigations*, the majority of all corporate data breaches are effectuated by organized criminal groups [22]. This Poneman Institute study puts the average cost for a data breach at $202 for each customer record compromised [23], and the pinnacle of severe data breaches has ended up costing approximately $109 million in the case of Heartland Payment Systems [24] (the sixth largest credit card processor in the U.S.) and $4.5 billion in the case of TXJ Companies [25] (the parent company of T.J. Maxx, Marshalls, and Home Goods). To compound this situation, with regards to the contacts receiving the spam, in the cases for which medicines are purchased over the Internet, approximately 50% of the pharmaceuticals have been found to be counterfeit [26].

These phenomena have prompted the realization that apart from contending with the baseline preexisting legalities for **cyber risks** as specified under the Family Educational Rights and Privacy Act (FERPA) of 1974, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Sarbanes-Oxley Act (SOX) of 2002, Federal Information Security Management Act (FISMA) of 2002, et al, the disciplinary scope of the cyber practitioner is broadening to encompass not just data breaches, but also risk management, supplier management, brand protection, perception management, and reputation management. This growing scope will very likely be accompanied by increasing liability associated with these expansion zones, such as product liability suits, even in those cases for which the company is simply a data breach victim. This is underscored by both the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act, which assert that companies are now responsible for bringing their supply chain partners into an overall compliance program [27]. Additionally, the degree of personal liability will directly correspond to the cyber practitioner’s day-to-day operational involvement and tangible actions of due care. After all, we now live in an era of elevated standards, whereby it is not just the *letter* of the law that is critical, but the compliance with the *spirit* of the law. Suffice it to say, this presents serious problems for the **cyber risk** professional.

In the realm of physical security, if something is really a big threat, you can typically see it coming — the rabid dogs coming over the other hillside or the army crossing the isthmus. You can readily see these threats, and they do not constitute a surprise. In the cyber security world, that is simply not the case. By way of example, if your car is stolen, you will notice. If your data is stolen, you still have it. If the police do an exceptionally good job, and your car reappears in your driveway, you know that no one else has it. But if your data has been stolen, you will never again be able to say whether or not someone else has a copy [28]. This poses an ongoing liability for companies experiencing data breaches. Given this operating environment of **cyber risk**, cyber security, information assurance, risk management, or whatever term of art one wishes to use, the arena is deemed to be an incredibly challenging intellectual field to engage in, because the problem space changes so rapidly. Even the recognized subject matter experts worry that, every day, something that was true yesterday might no longer be true today. Each and every day, the corpus of network-attached peripherals (e.g., uninterruptible power supplies, printers, copiers, postage meters, digital signs, point-of-sale systems, et al) is distending in size and its constituents are becoming increasingly computerized and subject to cyber attack (thereby constituting increased **cyber risk**). This interrelation of factors is depicted below in Figure 1.

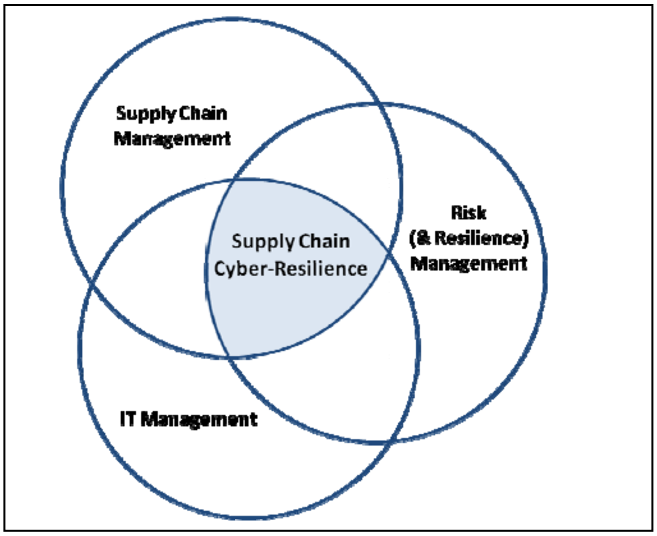

Figure 1. Main knowledge domains in supply chain cyber-risk management, Khan & Estay, Technology & Innovation Management Review, April 2015

The nexus between enhancing our **cyber risk** posture and increasing the transparency of the global supply chain is clear, as depicted above in Figure 1, and there are numerous researchers active in this space, including members of our team. First, cyber crime is the venue of choice for organized crime [29], particularly since the rule of law for Internet crime is — because of its transnational borderless nature — far more nebulous (e.g., there exists a non-unified motley crew of international treaties for extradition [30]) than conventional crime (traditional, illegal behaviors that most people think of as crime). Generally, Internet-facilitated spam and the sale of bogus goods carries with it penalties of up to five years of incarceration under the Criminal Spam Act of 2003 [31] and a similar tenure exists under the Anti-Counterfeiting Consumer Protection Act of 1996 [32], respectively, which by comparison, represent a much lower threshold of penalties than selling fifty grams of crack cocaine or ten grams of lysergic acid diethylamide (LSD), which carries a minimum of ten years imprisonment without parole under the Anti-Drug Abuse Act of 1986 [33].

Malware and spam are the tools of opportunity for organized crime, particularly since the draconian mandatory minimum sentences under the Federal Sentencing Guidelines Act of 1984 did not anticipate and take into consideration the combination of cyber crime/fraudulent drugs, particularly as the World Wide Web was not yet launched, until six years later, in 1990. Similar to how the odds in gambling are on the side of the casino, the advantage in the cyber landscape is currently skewed in favor of the criminal element. As an example, the average sentence for running an international multi-million pound counterfeit drug operation between 2002 and 2005 was 2.5 years imprisonment. Thus, since the penalty, even in the event of being successfully prosecuted, is comparatively speaking, much lower than other forms of crime, organized criminal groups have gravitated toward this very comfortable and prolific venue of fraudulent drugs — the flagship product promoted by the malware delivered by massive spam campaigns.

The profitability and growth of the counterfeit drug market is currently running rampant [35] and will continue to grow as a juggernaut force until this avenue of corruption has run its course and deemed to be no longer profitable for the currently engaged sophisticated criminal actors. For society to successfully transform the fraudulent drug business from a highly lucrative proposition to an unprofitable venue, the number of law enforcement seizures must increase to dramatically raise the cost of counterfeiting [36]; for these “Title 18” [37] busts to percolate quickly, there need to be more eyes from disparate communities of interest and many more voices from active public participation (such as in the manner consistent with the New York City Metropolitan Transportation Authority’s security slogan, and the now U.S. Department of Homeland Security’s mantra, “see something, say something” [38]).

IV. SEE SOMETHING, SAY SOMETHING FOR A MORE TRANSPARENT SUPPLY CHAIN

Since the time when Google acquired the geospatial data visualization firm, Keyhole, Inc., in 2004 and rebranded the Keyhole software offering, EarthViewer 3D, as Google Earth, the public interest in geographic information systems (GIS) and encompassing geospatial technologies has increased tenfold [39] [40]. Paralleling this phenomenon, the interest in utilizing network science tools and methodologies for better understanding the global supply chain has increased as well. Now, more than ever before, network science practitioners are eagerly observing and reporting various aspects of pedigree/provenance (i.e., the origin or source). This is critical for three reasons. First, in 2006, two hundred and sixty thousand bottles of Panamanian cold medicine contained antifreeze and killed at least one hundred seventy four people [41]. Second, in 2007, bottles of toothpaste bearing the Colgate and Crest brand, which contained substitute ingredients (e.g., diethylene glycol instead of glycerin) provided by a Chinese subcontractor killed at least a hundred people [42]; and third, in 2009, there was a massive peanut butter recall linked to salmonella poisoning, and the list of recalled products included a spectrum of items, such as peanut butter-flavored cookies, crackers, cereals, and ice cream [43].

Ultimately, this recall highlighted the complication of keeping food safe as it makes its way through a complex supply chain from farms to grocery stores shelves to kitchen pantries. Many have long advocated for transparency within the supply chain to provide the all-important origin or provenance information for the consumer [44]. After all, as customers, we want to know the pedigree of what we are buying and using, and of tantamount importance is authenticity. However, we are also concerned with ethics and environmental impact, as in 2006, when Gap, Inc recalled one of its clothing lines after an outcry that one of its Indian subcontractors was using children as young as ten years old to work sixteen hours a day for no pay [45]; and in 2010, when Nestlé fired one of its Indonesian suppliers after Greenpeace revealed that the supplier was destroying vast tracts of rainforests to make way for palm plantations, which produce the palm oil used in Power Bar, Coffee Mate, Nestle Crunch, and other Nestlé products [46].

THERE ARE 16 MILLION EYES IN THE CITY.
WE'RE COUNTING ON ALL OF THEM.
IF YOU SEE SOMETHING, SAY SOMETHING.
Tell a cop, an MTA employee or call 1-888-NYC-SAFE.

Figure 2. Example of New York City citizen vigilance campaign

So, what happens when the crowdsourced cylinders are all firing as in the example pictured above in Figure 2 amidst this era of a "Network Science Evolution" which is replete with a rich trove of geolocation and social media information, to help increase the overall transparency of the supply chain and combat counterfeit pharmaceuticals, et al?

V. Supply chain transparency for a breakthrough in cyber security

Imagine this. Given an increased number of tips from the "see something, say something" mantra and the resultant seizures, the counterfeit drug business is no longer as profitable [47], relative to other criminal venues. Hence, organized crime groups abandon this increasingly stringent sector, as their predominant revenue source, and the mass quantities of malware and spam begin to dip and suddenly fall away. With fewer professional **cyber risk** resources necessary for allocation towards the malware and spam amalgam, the new question becomes, "Does this constitute a breakthrough in governmental cyber risk efforts?" The answer is yes, absolutely [48]. After all, our current "state of the practice" cyber defense systems are not completely automated like science fiction writer Sir Arthur C. Clarke's sentient computer, HAL 9000. There still exists the necessity and significant reality of the all-important human component within human-computer interactions, and a finite amount of manpower necessitates careful prioritization in dealing with the Pandora's Box of cyber risk concerns. Given the newfound excess capacity of human cycles, other cyber risk domains are now able to receive an infusion of much-needed dedicated cycles of attention, thereby segueing into our penultimate question: "Exactly how significant are these newly allocated human cycles?"

Consider the following. When a historically proud seafaring nation, such as Great Britain, retires its flagship earlier than planned and begins to actively shrink the size of its surface warfare fleet so as to increase expenditures on cyber risk, you begin to sense that this new battle space is of serious concern. When you start digging into the classification of national threats within the U.K. and discover that the highest ranking national threat, a "Tier One," is assigned to a devastating attack on computer networks while a "Tier Two" threat is assigned to a nuclear, chemical, or biological attack, the sinking feeling in your stomach provides an indicator that something is afoot.

This begs the riveting question of whether the aforementioned freshly available human cycles can be of value-add to this endeavor? Absolutely, it can. The pathway of transparency within the global supply chain for the partial resolution of the cyber risk problem will be one that effectively makes counterfeit pharmaceuticals an unattractive venue for organized crime, and a lion's share of the world's spam and malware amalgams can indeed be remanded to the past.

To actually realize this vision and to effectuate a transparent supply chain so as to explore and contextualize the pedigrees of the innumerous ingredients and materials (which are sourced from around the world, aggregated, and processed to become the medicines we take, foods we eat, the clothes we wear, the things we buy, and the infrastructure we rely upon), we need to take a deep dive into the world of Big Data where there are branches and sub-branches of information pertaining to the trillion things that we have made in the world.

For this envisioned world, we cannot simply rely upon a centralized top-down identification and tracking system, which may be vulnerable to failure or being compromised by a cyber attack. We must engage the bottom-up distributed democracy, such as the nearly a billion smartphone users in the world, and situated before us now, we have the real possibility of leveraging the "Network Science Evolution" to contextualize the swarm of information from all over the world. This way, we can build a common operating picture of where our morning coffee comes from, whether anybody under the age of fourteen has labored to weave the clothes we are wearing, that the components of the aircraft we are flying today are of the highest standards of engineering excellence, and that the medicine we provide during humanitarian relief efforts are authentic.

VI. Conclusion

The earthquake-induced crisis in Haiti in 2010 was exemplary in showing the potential contribution of a complementary application of crowdsourced crisis mapping with standard disaster relief operations. Validation as well as bottom-up editing and management of geographic information were made easier and more rapid than in the past, but in parallel, limitations and challenges of data and information verification did indeed also emerge. Issues of veracity not only contaminated the information supply chain, but also expanded into the whole supply chain logistics that were part of the humanitarian relief efforts. As a result, a relatively large share of the pharmaceuticals supplied in Haiti consisted in fraudulent counterfeit medicinal drugs.

This case highlighted how crucial it is to expand our understanding of supply chain dynamics so as to reduce **cyber risk** as well as to improve disaster preparedness. Within this framework, the notion of transparency is, axiomatically, critical. Within large-scale product supply chains, transparency might only have a two-step depth, and in such cases, the likelihood of **blind spots** occurring increases exponentially. These blind spots can profoundly impact a country's economy, as is exemplified by the case of Japan and Toyota in the aftermath of the 1997 Aisin Fire [49].

It is evident that the there exists a nexus between the physical supply chain and the cyber supply chain, and it is clear that a stable economy and society does pass through the combined the enhancement of transparency of global supply chains and reduction of cyber risks. The case of fraudulent drugs promoted by criminal groups, via cyber attacks (e.g., through massive spam and malware campaigns) is paradigmatic of such nexus. Indeed, cyber attacks can not only include data breaches, impacts upon supply chain integrity, and other related attack vectors, but also represent a direct and profound danger to corporate reputation, particularly when the criminal group leverages a company's brand for nefarious purposes. Various governments have issued ad hoc laws stating that companies are now responsible for their entire supply chain, including partners; nevertheless, law enforcement is particularly arduous in the area of cyber crime, because the likelihood for criminal groups to be prosecuted is comparatively lower (given the Internets' transnational and borderless structure) and the possible penalty is much lower than other forms of crime.

The development of crowdsourced and participatory mechanisms for a more transparent supply chain is pivotal for identifying blind spots and mitigating their impact upon the integrity of supply chains. Concurrently, such efforts could reduce cyber risks in the digital world that currently represent a major threat to the stability of national and international economic systems. Thanks to the growing availability of crowdsourced and volunteered geographic information, more robust mapping and analytical tools have been developed and/or applied for bottom-up monitoring and mapping of socially or politically sensitive processes. Such results could represent the starting point to develop next-generation of network science tools, which lend to supply chain analytics, via pattern of life analyses, thanks to the integration of official and unofficial information produced (even involuntarily) across social networks and other collective intelligence feedback loops.

ACKNOWLEDGMENT

The authors would like to thank the Cyber Futures Center, an initiative of the Sensemaking-U.S. Pacific Command Fellowship, and the Dr. Steve Chan Center for Sensemaking — one of the centers of the Asia-Pacific Institute for Resilience and Sustainability (AIRS), which is jointly anchored at Swansea University's Network Science Research Center and Hawaii Pacific University — for the opportunity to study the challenges facing Hawaii and other archipelagos, and to contribute towards the various Public Private Partnership Initiatives aimed at developing solutions to overcome those challenges.

REFERENCES

[1] "Haiti Earthquake Victims to Receive $10 Million Worth of NYC's Counterfeit Goods," The Huffington Post 21 April 2010: 1.

[2] "Fatalities Associated with Ingestion of Diethylene Glycol-Contaminated Glycerin Used to Manufacture Acetaminophen Syrup," Center for Disease Control 2 August 1996: 1.

[3] "Counterfeit Internet Drugs Pose Significant Risks and Discourage Vital Health Checks," Science Daily 21 January 2010: 1.

[4] A. Gardner, "Fake Drugs Bought on the Web Pose Big Health Risks," U.S. News & World Report 29 January 2010: 1.

[5] A. Marshall, "The Fatal Consequences of Counterfeit Drugs," Smithsonian.com October 2009: 1.

[6] E. Clark, "Counterfeit Medicines: The Pills That Kill," The Telegraph 5 April 2008: 1.

[7] A. Coghlan, "Sawdust, Coffee and Dirt – Just About Anything Can End Up in Medicines Commonly Sold To The World's Poorest People. How Many More Will Die Before Proper Controls Are Put in Place?" New Scientist 29 March 1997: 1.

[8] S. Boggan, "Headache Pills Made of Rat Poison and Viagra Made of Chalk: We Reveal the Chilling Truth about Internet Drugs," Daily Mail 29 April 2009: 1.

[9] "Opening remarks by R. K. Noble, INTERPOL Secretary General," 2009 International Law Enforcement Intellectual Property Crime Conference 15 December 2010: 1.

[10] "Indian Start-up Strikes Deal to Combat Counterfeiting of Medicine," The Christian Science Monitor 14 December 2010: 1.

[11] "Counterfeit Drugs Pose Dangers in 90 Countries Worldwide," America.gov 14 October 2010: 1.

[12] Activities of the United Nations Office on Drugs and Crime to address emerging forms of crime," Conference of the Parties to the United Nations Convention against Transnational Organized Crime 18-22 October 2010: 15.

[13] J. Rothfeder, "Bumpy Ride," Portfolio.com 22 April 2009: 1.

[14] S. Narisi, "Feds Put IT in the Hot Seat for Security Breaches," Docucrunch.com 5 December 2010: 1.

[15] "Counterfeit Medicines," Novartis November 2005: 1.

[16] "The New World of eCrime: Targeted Brand Attacks and How to Combat Them," Mark Monitor March 2009: 1.

[17] "Organized Crime Wants Your Data," Docucrunch.com 5 December 2010: 1.

[18] L. Dignan, "Cyber Security by the Numbers: Malware Surges, Spam Declines in Third Quarter," ZDNet.com 17 November 2010: 1.

[19] "Expanded Study Finds More Insider Threats, Greater Use of Social Engineering, Continued Strong Organized Criminal Involvement," Verizon 28 July 2010: 1; Verizon's 2012 Data Breach Investigations Report.

[20] "Data Breach Costs Increase," Help Net Security 25 January 2010: 1.

[21] B. Krebs, "Payment Processor Breach May Be Largest Ever," The Washington Post 20 January 2009: 1.

[22] "Estimates Put T.J. Maxx Security Fiasco At $4.5 Billion," InformationWeek 2 May 2007: 1.

[23] "Growing threat from counterfeit medicines," Bulletin of the World Health Organization April 2010: 241-320: 1.

[24] S. Weber, "The U.K. Bribery Act 2010, Cheers!" Adfero Group 13 October 2010: 1.

[25] Interview with Dan Geer, Chief Security Officer for In-Q-Tel, the venture capital arm of the Central Intelligence Agency.

[26] B. Krebs, "Organized Crime Behind a Majority of Data Breaches," Washington Post 15 April 2009: 1.

[27] "UN Rejects International Cybercrime Treaty," ComputerWeekly.com 20 April 2010: 1.

[28] "Congressional Record-Senate," Congress 19 June 2003: 15564.

[29] "Trademark Counterfeiting – Introduction," Criminal Resource Manual 1997: 1701.

[30] E. E. Sterling," Drug Laws and Snitching: A Primer," Frontline, January 1999: 1.

[31] "U.K.'s Largest Counterfeit Drug Operation Concluded," Pharmaceutical Manufacturing 15 July 2009: 1.

[32] J. Schenker, "MPedigree's Rx for Counterfeit Drugs," Bloomberg Businessweek 3 December 2008: 1.

[33] "Report on Counterfeiting and Piracy in Canada: A Road Map for Change," The Canadian Anti-Counterfeiting Network March 2007: 39.

[34] E. Dou, "'See Something, Say Something' Goes National," Huffington Post, 1 July 2010: 1.

[35] GIS in Humanitarian Activities," Aid & International Development Forum 8-9 June 2011: 1.

[36] R. Hart, "Google Earth Popularity Booms," GeoCarta 25 January 2006: 1.

[37] "Panama Releases Report on '06 Poisoning," 14 February 2008: 1.

[38] J. Enoch "FDA Bans Toothpaste from China," ConsumerAffairs.com 24 May 2007.

[39] "How Does Salmonella Get in Peanut Butter? And Can You Kill It Once It's There?" Scientific American 13 January 2009: 1.

[40] Interview with Dr. Steve New, Program Director at the Centre for Corporate Reputation within the University of Oxford.

[41] "Gap: Report of Kids' Sweatshop 'Deeply Disturbing," CNN World 29 October 2007.

[42] D. Gutierrez, "Nestle Drops Indonesia Palm Oil Supplier After Greenpeace Report on Rainforest Destruction," Natural News 18 August 2010.

[43] "Fake Pharmaceuticals: How They and Relevant Legislation or Lack Thereof Contribute to Consistently High and Increasing Drug Prices," American Journal of Law & Medicine 22 December 2003: 1.

[44] Interview with Executive Director Maxim Weinstein, who leads StopBadware.org, a former Harvard Berkman Center for Internet and Society and Oxford Internet Institute project that develops new approaches to address malware.

[45] G. Wilson, "Fight Cyber War Before Planes Fall Out of the Sky," The Sun 19 October 2010: 1.

[46] M. Conner, "Sensors Empower the 'Internet of Things'," Electronics Design, Strategy, News 27 May 2010: 1.

[47] "One Billion Subscribers to Own Smartphone Devices in 2013," Informa 20 September 2010: 1.

[48] T. Nishiguchi and A. Beaudet, "The Toyota group and the Aisin fire," Massachusetts Institute of Technology Sloan Management Review, vol. 40, Fall 1998.