Center for Cyber & Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

# Strategic Insights Series:
## EUROPOL Executive Director Robert Wainwright

*Takedown of Dark Web Market Giants AlphaBay and Hansa*

July 2017

On July 20, 2017, the Federal Bureau of Investigation (FBI), the U.S. Drug Enforcement Agency (DEA), the Dutch National Police, and the European Union Agency for Law Enforcement Cooperation (Europol) jointly announced their coordinated takedown of the Dark Web market giants AlphaBay and Hansa — respectively, the largest and third-biggest criminal sites on the dark side of the Internet, which is password-protected, and where special software designed to mask its users is required for access.

The Dark Web is where criminal actors meet and transact, and where the black market in drugs, weapons, and other illicit goods & services thrives. The two sites that were seized in this case sold, among other things, illegal drugs, malware, and counterfeit documents; and provided illegal services. AlphaBay alone is estimated to have generated $1 billion (USD) in transactions since its inception in 2014. At takedown, there were over 350,000 listings for illegal drugs, goods, and services on AlphaBay. By comparison, the Silk Road (Dark Web) marketplace seized in 2013 had just 14,000 listings.

In order to learn more about this global law enforcement success, place it in broader context, and explore the lessons and implications for the future of cyber-policing, the Director of the Center for Cyber & Homeland Security (CCHS) at the George Washington University, Frank Cilluffo, spoke with Europol's Executive Director Robert Wainwright.

*Cilluffo: The scale, scope, and sophistication of this takedown were remarkable. Give us a sense of the sweep of this coordinated takedown by placing in context the importance of the Dark Web to criminals online and off, as well as the significance of the indicted actors and the illicit services they provided.*

*Wainwright:* Cybercrime is a key challenge for our digital economy and society because criminals quickly adopt and integrate new technologies into their modi operandi and exploit situations when the risk is low and the profit is high. Considering this, it was just a question of time until criminals discovered the Dark Web and therefore I am not surprised that in the last few years we have seen a continuous increase in criminal activity in dark market sites. The Dark Web is

becoming a haven for rampant criminality and the variety of illegal commodities available is something that can only be found online — can you imagine a physical marketplace where criminals can buy and sell 350,000 types of illegal goods from drugs and firearms, to credit card data, malware and counterfeit bank notes?

*Cilluffo: Tell us about the strategy and tactics adopted by law enforcement authorities in this case — including how officials managed to turn the "whack-a-mole" concept to advantage by monitoring the migration of AlphaBay users to another site when the primary marketplace was shut down.*

*Wainwright:* In the past we have seen how dark market sites taken down by law enforcement agencies have almost immediately been replaced by new marketplaces where vendors and buyers moved quickly to continue selling and buying illegal commodities. This can be frustrating, and we and our partners therefore decided to strategically exploit this criminal behavior. So, together we "lured the tiger off its mountain lair" as an ancient Chinese stratagem says, meaning never directly attack an opponent whose advantage is derived from its position. Instead, lure them away from their position thus separating them from their source of strength. This strategy magnified the disruptive impact of the joint action to take out AlphaBay and Hansa. It involved taking covert control of Hansa under Dutch judicial authority a month ago — which allowed Dutch police to monitor the activity of users without their knowledge — and then shutting down AlphaBay during the same period. It meant the Dutch police could identify and disrupt the regular criminal activity on Hansa but then also sweep up all of those new users displaced from AlphaBay, who were looking for a new trading platform. In fact they flocked to Hansa in their droves, with an eight-fold increase in the number of new Hansa members recorded immediately following the shutdown of AlphaBay. As a law enforcement strategy, leveraging the combined operational and technical strengths of multiple agencies in the US and Europe, it has been an extraordinary success and a stark illustration of the collective power the global law enforcement community can bring to disrupt major criminal activity. But the best strategy will not lead to success when there is no mutual understanding and cooperation between the involved partners. The outstanding success in the case at hand was only possible through the joint efforts of the Department of Justice, the FBI, the U.S. Drug Enforcement Administration, the Dutch Police and Europol.

*Cilluffo: Detail for us the special role of Europol in this case. What is its value-add and how does it go about supplementing and complementing the role of national authorities in the fight against cybercrime in particular? Also, elaborate upon the role of the private sector in this case and more generally; and explain how Europol works with the private sector.*

*Wainwright:* Frank, we are talking about two of the most active dark market places in existence. The combined criminal activity of these sites was huge and, therefore, several law enforcement agencies were actively investigating the sites, vendors and buyers. In order to be as effective as possible, it was necessary to coordinate and de-conflict all of these investigations. This coordination and supporting role is one of Europol's main activities. We have supported the investigations by facilitating the international police cooperation and secure information exchange, we have hosted operational meetings and we have analyzed and cross-checked the intelligence generated. In addition Europol sent intelligence packages to law enforcement partners across 37 countries, spawning many follow-up investigations across Europe and beyond. Some of the intelligence extracted contains relevant information regarding the destination of drugs and is meant to inform the relevant countries about planned shipments of drugs. Overall more than 38 000 transactions were identified by the Dutch Police since they took control and Europol sent more than 600 communications to its partners. This strategy was the outcome of months of work and discussion between the law enforcement agencies involved. At Europol we had numerous conference calls and operational meetings involving several law enforcement agencies to coordinate and align these actions.

*Cilluffo: What does this case portend for the future of online policing? What are the second- and third-order effects that you will be looking for, in order to better understand how the adversary will adapt and change their tradecraft? How can we build upon the successes of this case? Are there gaps or shortcomings that, from the standpoint of officials, still require remediation? And, how do we prevent criminal users of the Dark Web from ultimately regaining the upper hand, as new illicit marketplaces spring up to replace those that are taken down?*

*Wainwright:* The internet has become an essential and increasingly important part of our daily lives. It's an obligation for governments and law enforcement agencies to guarantee a safe digital environment for our citizens to enjoy. In my opinion, the internet is an instrument of freedom but of course capable of being exploited by criminals and terrorists. It is our job in law enforcement not to complain about difficulties but to protect the benefits and the freedom for our open societies. However, the online trade in illicit goods and services has been steadily expanding over recent years. I expect that this trade will continue to grow rapidly for the foreseeable future and that online platforms will emerge as a key distribution platform for all types of illicit goods in the EU. Of course the Darknet is a key facilitator for various criminal activities including the trade in illicit drugs, illegal firearms and malware, and only through the combined knowledge, expertise and capacity will the international law enforcement community be in position to tackle these threats, finding solutions for problems related to jurisdiction, access to e-evidence, encryption, anonymization or the use of cryptocurrencies. I believe that

the AlphaBay/Hansa case is a perfect model of coordination and joint international effort and it paves the way for future similar operations.

*Cilluffo: During the press conference about this case, you said the takedowns should serve as a signal to the adversary that they are not as anonymous on the Dark Web as they might think. Speak to the deterrent effect of this case — and to how law enforcement fits into a broader cyber deterrence strategy moving forward, rendering it more robust.*

*Wainwright:* Through the AlphaBay/Hansa operations, the capability of drug traffickers and other serious criminals around the world has taken a serious hit. By acting together on a global basis the law enforcement community has sent a clear message that we have the means to identify criminality and strike back, even in areas of the Dark Web. There are more of these operations to come. Despite the difficulties, law enforcement agencies will constantly work to identify criminals taking advantage of the Dark Web or technical tools. We first saw the Silk Road, and now AlphaBay and Hansa, fall. It's only a question of time before more administrators, vendors and buyers will be identified and prosecuted.

***Robert M. Wainwright*** was appointed Director of Europol in April 2009. He was reappointed for a second term in 2013, having overseen Europol's transition from intergovernmental organisation to EU agency status in 2010, ensured Europol's pivotal position in the new EU Policy Cycle for serious and organised crime from 2011, and secured the establishment of the European Cybercrime Centre (EC3) at Europol in 2013. Under his command Europol has also established the new European Counter Terrorism Centre and European Migrant Smuggling Centre, both in 2016.

## Contributors:

***Frank J. Cilluffo***, CCHS Director
***Sharon L. Cardash*** , CCHS Associate Director

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

**Website:** http://cchs.gwu.edu **E-mail:** cchs@email.gwu.edu **Twitter:** @gwcchs