Title: United in Necessity – Conditions for Cooperation Against Cybercrime

Author: Jobel Kyle Petallana Vecino

Institution: The University of California, Berkeley

Advisers: Vinod Aggarwal, Andrew Reddie, The University of California, Berkeley

Abstract: *Cybercrime continues to grow despite ongoing remediation efforts at the state and international level. The ease of access to commit cybercriminal activity beyond one's borders makes this an international issue. Examining the cooperative schemes provided utilized in intergovernmental institutions such as Europol helps illuminate the conditions which encourage states to cooperate to fight cybercrime. A study of these conditions may contribute to policy recommendations that will encourage further cooperation into the future.*

The problem of cybercrime continues to grow internationally; it is estimated to cost businesses globally an average of $6 billion per annum through the year 2021 (Eubanks, 2017). The ubiquitous nature of cybercrimes make them onerous to mitigate. The definition of cybercrime encompasses an extremely broad scope: it can be defined as acts or offenses “committed with the help of computer data and systems” (Fahey, 2014). A computer system can be anything from a personal mobile device to a large data center. Millions of people around the world have access to such tools; as of 2017, 3.79 billion people around the world utilize the internet (“Number of Internet Users” 2016). Any one of these users have the capability to commit cybercrimes only through internet access – there are countless other technologies that could be utilized to commit cybercriminal activity. Because tools utilized for cybercriminal activity are so widespread, states are constantly challenged to mitigate cybercrime on a massive scale. Furthermore, cybercriminal activity is transnational – an actor residing in one state can commit several criminal acts in another state. Due to these qualities, the fight against cybercrime is undoubtedly international.

In recent times, law enforcement agencies of different states have cooperated in order to pursue and reduce cybercrime. This cooperation has taken several forms. Some of these forms include ad-hoc partnerships, Memoranda of Understanding, intelligence sharing agreements, and joint operations. International law enforcement organizations, such as Europol, have established anti-cybercrime centers which facilitate cooperation between member states’ law enforcement agencies. However, while it is true that law enforcement agencies from different states cooperate with one another in various ways to fight cybercrime, it is unknown what conditions precipitate which types of cooperation. There is very little data on what compels a law enforcement agency to share cybercrime intelligence or to enter into a joint operation with another state's law enforcement agency.

This paper attempts to analyze three contentions. First, that law enforcement agencies of different states are more likely to cooperate with one another if institutional avenues for cooperation already exist. In other words, if an international institution exists and already facilitates forms of cooperation, states are more likely to utilize those avenues. Second, law enforcement agencies are more likely to cooperate with law enforcement agencies from other states due to the lack of a domestic information technology sector that employs a significant percentage of the population. Third, when law enforcement agencies cooperate across state borders against cybercriminal activity, this cooperation is most often to increase law enforcement agencies' capacities against cybercrime. This paper will utilize the existence of Europol as a case study and data gathered from law enforcement officials and agencies throughout Europe to show that Europol makes cooperation more likely.

First, this paper will review literature discussing the definitions of cybercrime, liberal institutionalist literature, and literature about European Union cybercrime policy. The research methodology of this paper will include two different types of interviews: qualitative interviews conducted with various EU policymakers and officials who focus on cybercrime and a short questionnaire completed by members from law enforcement units throughout Europe. The next section will analyze the results from these interviews and will present a typology of cooperative actions matched with their respective conditions. This typology will be analyzed to draw inferences for the conditions that lead to each type of cooperation, as well as policy implications for acts of international cooperation going forward, as well as discuss flaws and the potential direction for future research.

Contemporary Work on Cybercrime Cooperation

International cooperation to mitigate cybercrime has become a topic of interest for scholars of international cooperation and security cooperation since the late-2000s. The transnational nature of cybercrime establishes it as one of the most complex problems for policymakers to solve. The question of jurisdiction remains unanswered and commonly must be dealt with by states, non-governmental organizations (NGOs), and intergovernmental organizations (IGOs) ad hoc. Furthermore, the nature of cooperation remains opaque at best – some schemas are organized by shared traits among members while other schemas have their membership due to structural features that exclude other types of members (state-only organizations, for example). Lastly, in discussing how states cooperate with one another to fight cybercrime, one must consider the participation of NGOs such as Microsoft, Kaspersky, and Symantec, as states often rely on private sector partners to augment anti-cybercrime capabilities. So far, the literature focuses mostly on policy analysis related to the latter two subjects, without delving into the intentions or the conditions necessary for cooperation.

In Search of a Definition

Before proceeding with examining cooperation against cybercrime, one must first define the boundaries of what cybercrime actually is. Unfortunately, recent literature provides disparate definitions. In her piece discussing EU cybercrime and cybersecurity rule making, Fahey (2014) writes that a "comprehensive definition of 'cybercrime' for EU law has not been found in secondary law". She goes on to utilize Clough's definition of cybercrime: "offences against computer data and systems but also more broadly, to include offences committed with the help of computer data and systems". Fahey establishes cybercrime as a subset of cybersecurity, alongside cyberterrorism, cyberespionage, and cyberwar.

Bendiek and Porter (2013) utilize similar distinctions to Fahey but go further in detail. They note that international agreements on definitions are not only subject to technical and legal subtleties, but also cultural and political sensibilities over freedom of expression and government regulation. However they do note that distinctions are usually made, citing subcategories to cybersecurity similar to those that Fahey, but Bendiek and Porter provide more specificity to their definition. They define cybercrime as crime in cyberspace including "theft of intellectual property, the extortion based on the threat of DDoS (Distributed Denial-of-Service) attacks, fraud based on identity theft, and so on". However, they complicate this definition by including a "cyber-vandalism" category alongside cybercrime, which includes hackers defacing websites on the internet. Under Fahey's definition, the latter would fall under the umbrella of cybercrime. Furthermore, intellectual property theft may also fall under the subcategory that Bendiek and Porter exclude, cyberespionage. For the purposes of this paper, Fahey's definition would be most appropriate as it is all-encompassing.

Cooperative Schemas

Different cooperative schemes have been proposed by various scholars. On a macro level, Snidal and Vabulas (2013) discuss the distinction between formal intergovernmental organizations (FIGOs) and informal intergovernmental organizations (IIGOs). For this distinction, Snidal and Vabulas cite three primary factors: a formal treaty establishing an organization, three or more members within the organization, and the establishment of a formal secretariat to handle administrative duties. The authors go on to state that these distinctions are not set in stone and establish a spectrum between informal and formal IGOs, with many of their European Union examples falling somewhere between the two (Vabulas & Snidal, 2013).

Bendiek and Porter's characterization of European Union cybersecurity policy as a multi-stakeholder structure compliments Snidal's and Vabulas's work. Bendiek and Porter argue that the current division of responsibilities between civil defense, military defense, and law enforcement sectors to handle cybersecurity, and specifically tackle cybercrime, have faltered. There exists far too much cross pollination of threats and responsibilities for any one sector to handle these threats on their own (Bendiek & Porter, 2013). In practice, this seems to inform the nature of cooperation between entities against cybercrime – informal or ad-hoc interactions between states and state institutions arise. These informal interactions could potentially be categorized in Snidal's and Vabulas's spectrum as informal IGOs. However Bendiek and Porter do note that these interactions seem to be evolving into progress toward formalized institutions – they specifically cite the example of Europol's European Cybercrime Center (EC3) in conjunction with the cross-border prosecution organization Eurojust as steps toward international coordination against cybercrime (Bendiek & Porter, 2013). As this paper will be focusing on Europol as a case-study, the following paper will examine the conditions necessary for cooperation against cybercrime within a formal structure.

Dupont's (2016) work goes as far as to map interactions between states and organizations in the context of cybercrime to specific classifications. Dupont utilizes network analysis to build visual networks through which to show how states and organizations interact with each other to fight cybercrime. The overwhelming majority (74.5%) of initiatives he includes in his dataset involve capacity building, though information/intelligence exchange characterize 49% of these initiatives as well. Dupont concludes from his analysis of the cooperation networks that cooperation seems to occur due to a specific issue – for example, one of the clusters consists of links between institutions and NGOs that are interested specifically in stopping child abuse.

Other points of interest include the smaller amount of connections states known for sponsoring cybercriminal activities such as Russia and China have in comparison to other states. However Dupont professes that these connections do not show the intensity of the cooperation between states and NGOs in fighting cybercrime or the intentions behind their cooperation. He also goes on to state that the data used in his paper does contain biases: it is "limited to multilateral initiatives, and methodological similar bilateral arrangements for cooperation or investigations police forces conducted in recent years under the impetus of the FBI and Europol would certainly produce a significantly different image" (Dupont, 2016). Because this paper will be focusing on operations undertaken under the aegis of Europol, it would be prudent to utilize this data to assess Dupont's categorizations.

Lastly, Jamil's (2012) work on the Budapest Convention on Cybercrime illustrates various reasons why states may or may not join formalized cooperative schemes. Some of these concerns include a centralization of power in a specific region. Some states choose to forego one cooperative scheme in favor of another, due to how a scheme may market itself (i.e. internationally-based versus regionally based). Dupont echoes the latter findings in his network analysis, with some organizations attempting to outmuscle each other due to duplicate focuses. These produce separate and competing networks of cooperation with one network consisting of members exclusive from others (Dupont, 2016). Taking these concerns into perspective informs an analysis of the usage of an intergovernmental police organization which may duplicate national crime agency functions such as partnerships with non-governmental technology partners and investigation procedures.

The Public-Private Partnership

A large trend that many of the pieces harp on is the emergence of NGOs as actors in cooperative schemes against cybercrime. Bendiek and Porter argue that as new political paradigms form in the fight against cybercrime, the distinction between the public and private sectors breaks down. Because private organizations are now responsible for large amounts of critical infrastructure in Europe including healthcare and energy, they are now targets for cybercriminals. Their inclusion in fighting cybercrime is essential (Bendiek & Porter, 2013). Moreover, Dupont notes that other private firms such as Microsoft and Symantec have more capability in fighting cybercrime than many states do. As such, their inclusion in cooperative networks has become essential and organizations attempting to build cybercrime cooperation including Interpol and Europol have gone as far as to include corporations as partner organizations to build more capacity and access private firm capabilities (Dupont, 2016). Tropina (2015) argues that continuing to establish informal relationships between the states and these private firms, as the establishment of uniform compliance procedures could hinder the effectiveness of these private firms as partners against cybercrime. Bossong and Wagner (2017) disagree with Tropina and insist that formalized agreements support the effectiveness of public-private partnerships. However through application of a cross-cutting analysis, they also find that public-private partnerships are often only rhetoric and cooperation of this kind is not usually in the interest of private firms, therefore leading states to push toward regulating industry organizations (Bossong & Wagner, 2017). This last observation seems to line up with the trend that Tropina was noticing as well; however due to the contemporaneousness of the latter article it seems clear that the regulatory trend continued beyond 2015 and may seem to be the only recourse for states in keeping private firms in the fold.

The literature so far has shown plenty of disagreement in many places. Due to the burgeoning nature of cooperation against cybercrime, it seems somewhat safer to rely on latter works as the landscape has easily transformed within the course of just a few years. Dupont's network analysis is the closest any of the scholars have come to discussing the conditions under which states interact with one another in order to tackle cybercrime though it is extremely curious to note that he omitted Europol interactions, which should be prevalent among European states. Nevertheless, despite Europol's existence as a facilitator for anti-cybercrime cooperation, one must note that many of the interactions between law enforcement groups within member states occurs on the local or regional level rather than the state – in other words, these interactions may be closer to constituting IIGOs than FIGOs despite the existence of a formal organizational structure and treaty acceded to by state governments. Lastly, despite Bossong and Wagner's findings that private firm cooperation against cybercrime is only skin-deep in many cases, one must take into account Dupont's argument that some private firms have better anti-cybercrime capabilities than some states do. It remains pivotal to take into account the impact private firms can have on state-level cooperation against cybercrime.

European Police Agency Anti-Cybercrime Operations

The following section will discuss findings from interviews conducted with Europol's European Cybercrime Center (Europol) Head of Strategy Philipp Amann (Amann, 2018) as well as interviews conducted with the United Kingdom National Crime Agency. The following section will also include findings on different metrics of cooperation will be presented from the results of a ten-question questionnaire presented to the national crime agencies of the United Kingdom and Denmark.

Europol's operations consist of three primary categories. These categories include operational support, including intelligence sharing, analysis, and on-the-ground support, education and awareness training, and coordinating or taking part in multilateral/joint actions. Intelligence sharing serves as the primary day-to-day work that Europol undertakes. Much of this intelligence sharing occurs on the Secure Intelligence Exchange Network Application (SIENA), a platform through which law enforcement agencies from Europol's member states as well as Europol officials and third-parties with cooperation agreements with Europol can communicate and disseminate intelligence to other partners or to Europol itself. Europol also conducts malicious software (malware) analysis through the Europol Malware Analysis System (EMAS) (Amann, 2018). Member state agencies can submit a piece of malware and Europol employees can conduct forensic analysis on the malware to produce conclusions and support a member state in their investigation or an active operation. Member states also have access to the Digital Forensics and Mobile Laboratory, which mines data from hard drives or mobile phones, and Europol's decryption platform, which can decrypt user passwords with a 68% success rate (NCCU Research, 2018). Lastly, Europol interfaces with outside partners including Interpol and third-party states, as well as non-governmental partners including private firms, accepting information from them including IP addresses as well as consulting non-governmental partners in an advisory capacity (Amann, 2018).

Based on the interview with Amann, there seems to be evidence that complicates the primary findings derived from the literature, in particular Dupont's findings that capacity building makes up the overwhelming plurality of cooperative interactions against cybercrime (Dupont 2016). Specifically, Amann ranks the following cooperative actions against cybercrime in order of primacy from least to greatest: education and prevention outreach, intelligence sharing and operational support, and joint actions and operations. Amann also ranked the three types of cooperation in terms of frequency from least to greatest: education and prevention outreach, joint actions and operations, and intelligence sharing and operational support. If one categorizes capacity building as education and prevention outreach, then in both metrics of importance and frequency, capacity building is seen as both least important and least frequent. If one categorizes operational support (in particular, intelligence sharing and analysis) as part of capacity building, then capacity building becomes both most important and most frequent (Amann, 2018). However, operational support would not include common actions associated with capacity building such as education. Admittedly, Amann emphasized that the difference in importance between these three actions are minimal and the relationship between the three is close and each type of cooperation is often tied to another type of cooperation. Other avenues for operational support include Europol's Joint Cybercrime Action Taskforce (J-CAT), a team of international investigators that coordinate international operations (NCCU Research, 2018). Officers are sometimes sent from member state crime agencies to work on specific cases if necessary. Based on this evidence, there exists ample opportunities for states to request operational support among other types of actions, although intelligence sharing does make up the bulk of the day-to-day work. However, even though opportunities for cooperation to engage in operational support against cybercrime exists, Europol's structure does not necessitate compulsory participation from member states.

The organizational structure of Europol is far-less hierarchical and tends to be driven by voluntary cooperation. Amann notes throughout the interview that Europol would not directly inform a member state that their protections against cybercrime require improvement unless the state in question asked Europol for an assessment. Any of the intelligence shared by member states (including open source reports, malware, and other forms of data) is submitted by on a voluntary basis (Amann, 2018). Should a member state choose not to share their intelligence, Europol cannot force a state to share that intelligence. Even with the voluntary nature of national crime agencies' relationship with the institution, Amann remarked that the member states do utilize Europol effectively. Thus, unlike what neoliberal institutionalist literature (Snidal, 1985) would suggest, states do not require negative reinforcement to cooperate with one another against cybercriminal activity. This may be due to the transnational nature of cybercrime necessitating cross-border investigations to apprehend perpetrators.

Despite cooperation being to some extent voluntary, Europol provides trainings, funding, and pursues policy objectives. Free anti-cybercrime tools such as forensic analysis tools developed through the FREETOOL project are provided to member states. Much of its educational outreach and operational support focuses on establishing a baseline level of expertise among member states to ensure effective cross-border cooperation (Amann, 2018). Policy plans known as European multidisciplinary platform(s) against criminal threats (EMPACT cycles) dictate Europol's policy objectives and help determine which targets the organizational pursues and the kinds of operations it chooses to undertake. Therefore utilizing Europol as a platform for cooperation does involve adopting predefined policy procedures and objectives that may not line up with a member state's chosen policy objectives. However, states have the ability to influence these policy objectives if they choose to provide input into their formation and adoption (NCCU Research, 2018). Europol also provides funding to member state agencies to implement policy objectives; this funding can also be used to implement joint projects international projects proposed by member state agencies (Amann, 2018).

When attempting to isolate the reasons why a member-state agency would not cooperate with Europol, Amann states that member state law enforcement agencies are often either unaware or ignore the resources Europol can provide. In fact, Europol officials are aware that member states have law enforcement agencies that are producing tools and materials that the organization has already produced (Amann, 2018). According to Amann, this is primarily due to law enforcement agencies across member states being unconscious of what Europol can provide those agencies. Rather than pursuing policy-based prescriptions to bring these agencies into the fold, Amann suggests that Europol needs to do a better job of advertising and outreach to these law enforcement agencies. The choice to attribute the perception that Europol lacks usefulness to member states to lack of outreach rather than tying it to the legal frameworks that member states must ratify in order to maintain membership seems to indicate either an unwillingness to establish a more hierarchical structure or a belief that a more hierarchical structure is unnecessary.

In the context of public-private partnerships, Europol maintains relationships with public-private partners for operational and advisory purposes. Non-governmental organizations provide Europol with intelligence including IP addresses of potentially compromised or potentially suspicious computers (Amann, 2018). Non-governmental organizations are also utilized in an advisory capacity through membership with an advisory board. Amann remarked that it is likely that most member states would hold their own relationships and partnerships with non-governmental organizations. These partnerships are usually not kept track of by Europol; thus the relationship between member states and EC3 is less hierarchical despite the fact that institution policy drives the direction of the relationship (Amann, 2018). The British National Cyber Crime Unit (NCCU) remarked that business costs and potential to negatively impact reputation often stand in the way of forming partnerships with non-governmental organizations. However, NGOs seem to be willing to share more information on some types of attacks, such as DDoS attacks, due to lower reputational risks in comparison to attacks that disclose user data (NCCU Research, 2018).

Further findings include questionnaire results from the Danish National Cyber Crime Center (NC3). The questionnaire consisted of nine multiple choice questions focusing on various topics including funding from Europol for anti-cybercrime operations, frequency of interactions with Europol in the context of anti-cybercrime operations, and frequency of interactions with domestic and international non-governmental technology partners, and one free-response question focusing on an agency’s comparative capability to Europol’s. These figures have been recorded in Table 1.

All results refer to the most recent year unless noted otherwise	
Trainings requested from Europol	2
Funding requested from Europol for anti-cybercrime operations	€0
Percentage of anti-cybercrime operations that require direct operational involvement from Europol	1-20%
Percentage of private technology partners that also have partnerships with Europol	1-20%
Percentage of total interactions with private technology partners through Europol	1-20%
Percentage of interactions with domestic private technology partners	41-60%
Percentage of interactions with EU-member state police agencies through Europol	21-40%
2016 ICT sector employment percentage compared with average Europol member state 2016 ICT sector employment	+0.6%

Table 1*: Danish NC3 interactions with Europol and other anti-cybercrime partners*

These results are striking as they indicate that the overwhelming majority of cybercrime operations do not require direct operational involvement from Europol. When measuring Information Communications Technology (ICT) sector-size as a percentage of total employment within Denmark, Denmark has above-average ICT sector employment in comparison to the rest of the Europol member states. Nevertheless, in a comment at the end of the survey, the agency stated that “the resources and capability of the member states…holds back the common process. Cyber [crime] has to be prevented and fought from an international perspective” (NC3, 2018). From this statement, one can surmise that while this specific crime agency may not interact with Europol to handle the vast majority of their anti-cybercrime operations, the international nature of cybercrime places a premium on platforms for international anti-cybercrime operations.

One confounding variable that arose from the data collected through interviews and surveys is the cultural role of police in cybercrime investigations. Amann suggested that several Europol member states would have different cultural attitudes toward policing that would affect their willingness to cooperate internationally with other law enforcement agencies or with non-governmental partners. He brought up the example of the Netherlands, where many of the banks have close partnerships with anti-cybercrime initiatives and policing agencies; Dutch banks interface with anti-crime task forces to disseminate information with other banks and law enforcement representatives in the same room (Amann, 2018). Amann claims that these partnerships would not be tolerated by citizenry of other member states due to cultural and social views on privacy and police activity in those member states. The legal frameworks of these countries also factors into whether these types of cooperative relationships would be possible.

Another confounding variable that was brought up in the interview was the size of the country’s bureaucracy. Again citing Estonia, Amann noted that the country itself is small in population and does not encounter the same amount of bureaucratic complexity that a larger member states such as Germany or France. The lack of bureaucratic complexity leads to a reduction in formal structures compared to larger countries, leading to a smaller amount of people taking on a larger amount of responsibilities. This increases speed and responsiveness of the relationship government officials of these smaller countries have with Europol at the cost of higher barrier to establishing relationships when government officials first take office (Amann, 2018). In contrast with Estonia, the Netherlands has many formalized structures for partnerships with Europol which creates a different approach and platform for cooperation. Bureaucratic turnover also creates problems. The constant turnover of senior management staff of Europol member states leads to a lack of institutional memory among government staff and policymakers (NCCU Research, 2018). This turnover may result in a new staff that does not know how to utilize Europol resources effectively and/or efficiently.

Conditions to Cooperation

Europol’s pre-existing structure and the decision to expand into the realm of cybercrime may have given it the ability to establish its capabilities to the point that supersedes member-state capabilities. When asked whether NC3 could claim equivalent anti-cybercrime capabilities to Europol, the police agency responded “No” (NC3, 2018). Europol’s preexistence is an important detail to note; Europol was established in 1998 but did not establish a dedicated cybercrime operations unit until 2013. The establishment of the organization predates many of the member-state cybercrime agencies, only some of which, such as Greece, predates the establishment of Europol. Europol’s establishment of a European Cybercrime Center predates several member states’ cybercrime agencies; Greece’s anti-cybercrime unit predates Europol’s existence, having been established in 1995 (Chrysopoulos, 2016). However many of the other member state units, such as Austria’s and the United Kingdom’s, were established after 2000. While Europol’s dedicated cybercrime center postdates many of the member-state agencies, states do not seem to feel the need to deviate from Europol’s pre-established framework. If there already exists an organization that can serve as a niche for a form of cooperation, as in the case of Europol and EU-wide crime response, there may be less overhead required to convince member states to engage in new forms of cooperation. The remark made by the NC3 indicates that Europol's known reputation and ability entices states to approach the organization with some degree of confidence.

When attempting to ascertain whether international cooperation against cybercrime focuses on capacity building, it may be useful to categorize the different types of cooperation. Dupont's analysis for different forms of cooperation can be used as a framework (Dupont, 2016). From the data gathered from the interviews and survey mentioned in the previous section, the different kinds of cooperative actions against cybercrime can be characterized in Table 2.

Category of Action	Action/Operation
Capacity Building	• Trainings and educational services • Monetary funding • Technical forensics analysis tool development
Exchange of Information	• Intelligence exchange through SIENA • Technical forensics analysis tool usage
Law enforcement operations	• Investigations supported by Europol personnel • Joint investigations between member states • Technical forensics analysis tool usage
Lobbying	• Ability to influence Europol policy objectives

Table 2*: Categorization of Anti-Cybercrime Cooperative Activities*

Given that intelligence sharing makes up most of Europol's day-to-day work, it seems reasonable to conclude that exchange of information trumps all of the other categories. This conclusion is not necessarily predicated upon the inclusion of technical forensics analysis tool development, as SIENA still constitutes the bulk of intelligence report sharing. Figure 2 shows that the categories Dupont lays out does not cleanly classify the different types of cooperation; there exists overlap in some of the categories depending on the type of action. For example, as an open-source project, the development of the FREETOOL project can be considered capacity-building to allow member state police agencies to augment their cybercrime analysis capacity. In contrast, tools such as EMAS are only useful if other states share their malware through the system. However, both allow member states to build up their capacity to analyze malware. Furthermore, in his interview, Amann characterized the use of such tools not as capacity building but as operational support, placing technical forensics analysis tools under the category of law enforcement operations. This overlap makes it difficult to provide a discrete category for each type of cooperation. If one were to categorize capacity building as funding, education, and capability development, then capacity building would come in third to information exchange and law enforcement operations, respectively.

Based off of these findings, it is reasonable to posit that while capacity building does play an important role in anti-cybercrime cooperation, member states may not focus primarily on it if an organization is capable of facilitating more direct means of engaging potential threats. The Danish National Cybercrime Center's survey responses are very telling in this regard. The center did not request funding for anti-cybercrime operations in the 2017 fiscal year. However, the center also noted that up to 40% of interactions with other EU member-state crime agencies required interaction with that agency through Europol and up to 20% of anti-cybercrime operations required direct involvement from Europol (NC3, 2018). Despite neither of these making up the majority of their respective types of operations, they still occur at regular enough frequency to be considered the primary work of Europol. Furthermore, both intelligence sharing and law enforcement operational support directly engage potential cybercriminal threats, whereas capacity building would have a peripheral influence on mitigating cybercrime. Based on this evidence, it seems that a condition conducive to pursue cooperation to execute operations requires the existence of an organization that has a known and trusted operational structure.

When comparing ICT employment percentages compared to the average EU employment percentage, the Danish response to the survey is also provides illuminating data. Denmark contains ICT employment that is above the EU average for ICT employment as a percentage of total employment for the entire country (European Commission, 2016). The Danish National Cybercrime Center also remarked that up to 20% of interactions with non-governmental technology partners occur through Europol. Around half of the agency's interactions with non-governmental technology partners occur domestically, which does not require interaction with Europol to access. Prima facie, all of these points would lead one to suspect that such a state would be less dependent on Europol's potential opportunities for access. Nevertheless, it seems that even a relatively small need to fight potential cybercrime threats coming internationally results in a willingness to engage in cooperative activities regardless of the volume of problems those activities can solve. This leads one to conclude that an intrinsic property of the problem, cybercrime's international nature, serves as a primary motivator behind states' willingness to cooperate to fight it, and other potential avenues for mitigation, specifically domestic avenues, are not enough to make a state's police agency feel secure.

Next Steps

This paper has examined three contentions: if a prior institution already exists, states would be more likely to cooperate within the realm of a new issue area, that if a state did not have a strong domestic technology sector, its police agencies would be more willing to cooperate internationally to fight cybercrime, and if cooperation against cybercrime does occur, it will most likely be to build capacity within state agencies to combat cybercrime themselves. Given the evidence presented from this piece, only the first contention continues to hold strong. Europol's prior space within the realm of international police agency cooperation seems to have spurred states to engage in cooperation with other states through the organization and with Europol personnel themselves even if states established a cybercrime unit that preexisted EC3. Contributing to this willingness to cooperate also seems inherent to the problem of cybercrime; that is, effective mitigation must be international in scope. The other two contentions, however, falter. As seen in the case of Denmark, an above-average ICT sector size in terms of percentage of employment does not lessen the value that its cybercrime unit places on Europol's utility in fighting cybercrime. Observations of the types of support that Europol gives also seems to focus readily on operational support and information exchange, effectively supplanting capacity building as the top type of interaction. Again, it seems that reputation and ability play directly into how states utilize Europol. The organization's structure and services lends itself to direct support of law enforcement operations. The ability to provide known, effective services can be construed as a precondition to states cooperating within an IGO on an operational basis.

This project is currently ongoing – data from other Europol-member state police agencies must also be taken into account before drawing further policy implications. This current version of this project only observes two states which both have higher-than-average technology sector size in terms of ICT employment percentage. The next step would be to see if another state that has lower-than-average technology sector size will provide similar data to those of the states examined so far. Furthermore, it is important to note that there are no competing IGOs or NGOs that have codified intelligence-sharing agreements and anti-cybercrime capabilities to the extent that Europol has. Therefore, it is difficult to discern if the organization is seen as effective due to a lack of available comparison with other organizations or if it is truly due to the organization's performance. This paper also does not necessarily develop a direct causal link behind some of its proposed preconditions and the conditions themselves, as the lack of a competing agency without Europol's reputation cannot be tracked to measure its utilization. Nevertheless, the preconditions of reputation and known competence must be taken into account as an important consideration should IGOs and NGOs want to encourage international members to cooperate, whether against cybercrime or some other matter of international security. In his interview, Amann summed up the biggest factor in one word: "trust". It is not just trust in one's partners, however; it is trust that cooperation will lead more often than not to a successful operation. This indicates that the overhead necessary to convince states to cooperate is very large, but once that overhead is met, states will not need much convincing in the future.

Bibliography

Amann, P. (2018, January 8). Interview with Philipp Amann, Head of Strategy, European Cybercrime Center [In-Person].

Bendiek, A., & Porter, A. L. (2013). European Cyber Security Policy within a Global Multistakeholder Structure. *European Foreign Affairs Review*, *18*, 155.

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3

Chrysopoulos, P. (2016, February 18). Greek Police Transfers Cyber Crime Unit Chief, Then Repeals Decision, Then Transfers Him | GreekReporter.com. Retrieved March 19, 2018, from http://greece.greekreporter.com/2016/02/18/greek-police-transfers-cyber-crime-unit-chief-then-repeals-decision-for-now/

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. *Cultures & Conflits*, (102), 95–120. https://doi.org/10.4000/conflits.19292

Eubanks, N. (2017, July 13). The True Cost Of Cybercrime For Businesses. Retrieved December 13, 2017, from https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/

European Commission. (2016, August 11). Eurostat. Retrieved March 19, 2018, from http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables

Fahey, E. (2014). *The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security* (SSRN Scholarly Paper No. ID 2384491).

Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2384491

NC3. (2018, March 16). Interview with Danish National Police Cyber Crime Center [Text].

NCCU Research. (2018, February 21). Interview with United Kingdom National Cyber Crime Unit [Text].

Number of Internet Users (2016) - Internet Live Stats. (n.d.). Retrieved December 12, 2017, from http://www.internetlivestats.com/internet-users/

Snidal, D. (1985). The Limits of Hegemonic Stability Theory. *International Organization*, *39*(4), 579–614.

Vabulas, F., & Snidal, D. (2013). Organization without delegation: Informal intergovernmental organizations (IIGOs) and the spectrum of intergovernmental arrangements. *The Review of International Organizations*, *8*(2), 193–220. https://doi.org/10.1007/s11558-012-9161-x