United by Necessity: Conditions for Institutional Cooperation against Cybercrime

Jobel Kyle P. Vecino
Charles and Louise Travers Department of Political Science
University of California, Berkeley
Berkeley, California, USA

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 utilized in intergovernmental institutions such as the European Union (EU) Agency for Law Enforcement and Cooperation (Europol) illuminates possible conditions that encourage states to cooperate to fight cybercrime. Testing these conditions shows that the preexistence of an institution in a related issue area serves as the strongest driver of cooperation within an international institution against cybercrime.

Keywords– cybercrime; cybersecurity; Europol; institutions; international cooperation

I. INTRODUCTION

The problem of cybercrime continues to grow internationally; according to estimates, it will cost businesses an average of $6 billion per annum globally through the year 2021[1]. Some states have greater capabilities to handle cybercrime than others. In some cases, multinational corporations and academic research institutions wield stronger cybercrime mitigation capabilities than some states. The ubiquitous nature of cybercrime also makes it onerous for any one state to fight cybercriminals alone. Recently, national law enforcement agencies began to participate in newly-formed international institutions focused on cybercrime mitigation; Europol serves as one example. What qualities or conditions drive states to cooperate within these institutions to fight cybercrime? I seek to identify these qualities or conditions in order to draw policy implications that will encourage further cooperation among states in the realm of international security.

This paper analyzes three contentions. The first is that law enforcement agencies of different states are more likely to cooperate with one another if institutional avenues for cooperation already exist. This paper refers to this type of cooperation as "iterative cooperation." Second, law enforcement agencies are more likely to cooperate within an organization to remedy a lack of, and inability to develop, domestic technical expertise in fighting cybercrime. This paper categorizes this type of cooperation as "cooperation by substitution," in that the states utilize the institution's capacities in lieu of their own due to an inability to develop those capacities. Third, if the majority of cooperative actions through organizations such as Europol can be characterized as capacity building, states cooperate within the institution to establish self-sufficiency in anti-cybercrime operations. This paper refers to this type of cooperation as "cooperation for self-reliance." This paper capitalizes on the existence of Europol as a case study and data gathered from law enforcement officials and agencies throughout Europe to demonstrate that iterative cooperation through prior interactions represents the most important driver in what compels states to cooperate within an institution against cybercrime.

A. Europol and the European Cybercrime Center (EC3): An Overview

Europol is an EU agency headquartered in The Hague, Netherlands. It primarily concerns itself with assisting member states in fighting crime and terrorism by providing member state law enforcement agencies with a mechanism for the facilitation of secure intelligence exchange, primarily concerning internal security matters[2]. Europol also coordinates cross-border anti-crime and anti-terrorist operations with member states' law enforcement agencies and interfaces with outside partners, collects open-source intelligence and intelligence procured from publicly-available sources, and creates analyses from both intelligence provided by member states and intelligence collected by the agency[3]. All participating states are members of the EU. Non-EU-member state partnerships are either considered "operational" or "strategic." Operational partnerships allow for information exchange between partners and Europol, including the exchange of personal data. Operational partners include Australia, the United States, and the International Criminal Police Organization (Interpol)[4]. EU partners can access more of Europol's services than non-EU partners can, with participating EU member states having the most access.

Member status in Europol is dependent upon state ratification of EU regulations relating to home and justice matters[5]. However, participation in the organization is noncompulsory for EU member states. Europol does not have the power to mandate participation; if one state decides to share its intelligence on cybercrime, it does not have the political authority to force all other member states to also share their intelligence. Therefore, many of the actions undertaken by Europol member states within the context of the organization are entirely voluntary. Policy plans known as European multidisciplinary platforms against criminal threats dictate Europol's policy objectives and help determine which targets the organization pursues and the kinds of operations it chooses to undertake[6]. 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[7]. This makes Europol a useful case study for analyzing conditions that lead to anti-cybercrime cooperation without some form of hierarchical enforcement.

This paper in particular focuses on participation within Europol's EC3, which provides many of Europol's base intelligence sharing and analysis functions, specifically for the purpose of fighting cybercrime[8]. With regard to technical provisions, the institution provides tools and technical analysis to aid in investigations against cybercriminal activity, such as malware analysis, technical capability development, and the ability to decipher passwords with some success[9]. EC3 may also provide member states and member state police agencies with funding as well as educational support in the form of training and seminars[10]. Finally, EC3 (through Europol) also holds relationships with private firms[11]. This paper refers to Europol and EC3 as the same entity (Europol) as Europol houses EC3, membership does not vary between the two, and Europol member states and EC3 staff have access to other Europol functions and vice-versa.

II. CONTEMPORARY WORK ON CYBERCRIME COOPERATION

A. In Search of a Definition

Before examining cooperation against cybercrime, the term "cybercrime" must first be defined to shed light on the nature of the problem. Elaine Fahey writes that a "comprehensive definition of 'cybercrime' for EU law has not been found in secondary law"[12]. She goes on to utilize law professor Jonathan 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"[13]. Fahey establishes cybercrime as a subset of cybersecurity, alongside cyberterrorism, cyberespionage, and cyberwar. Because tools utilized for cybercriminal activity are so widespread, states are constantly challenged to mitigate cybercrime on a massive scale. Annegret Bendiek and Andrew L. Porter present a competing 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"[14]. However, they complicate this definition by including a "cyber-vandalism" category separate from cybercrime, which includes hackers defacing websites on the internet. Under Fahey's definition, the latter falls under the umbrella of cybercrime. For the purposes of this paper, Fahey's definition is the most appropriate, as it is all-encompassing, and Europol characterizes cybercrime similarly in its threat assessments[15].

B. Cooperative Schemes and Institutional Choice

Because Europol consists of many member states but holds no authority over those states, classifying Europol as an intergovernmental organization (IGO) is appropriate; however, dis-

cerning the type of IGO provides greater insights into how states are compelled to cooperate within its auspices. Using Felicity Vabulas' and Duncan Snidal's classifications, Europol could be described as a formal IGO (FIGO), an organization established by a formal treaty (as a provision of the Treaty of Lisbon) which consists of three or more members and contains a formal secretariat to handle administrative duties[16]. Thus, cooperation that focuses on Europol is subject to the same conditions that drive states to cooperate within FIGOs generally.

Kenneth Abbott and Snidal cite that two features of FIGOs make them attractive to states: centralization and independence[17]. Centralization refers to the idea that institutional tasks are handled by a singular focal entity[18]. In the case of Europol, these tasks include technical analysis, intelligence dissemination, public-private partnership facilitation, and operation coordination. Centralization facilitates the pooling of these activities as transaction costs and logistical overhead can be reduced through the use of the organization's staff, allowing all member states to share some of the burden and reap the reward of Europol's technical expertise or intelligence reports[19]. Abbott and Snidal also suggest centralization allows for easier management of joint production activities, which in this context could constitute anything from the production of common anti-cybercrime policy to the coordination of joint anti-cybercrime operations[20]. The independence of Europol also allows for the neutral distribution of funds and dissemination of intelligence through the organization. Both centralization and independence enable organizations to handle a large volume of work and manage complex operations, the benefit of which, given the scope and intricacy of cybercrime, cannot be understated.

But why choose to augment an existing formal institution instead of creating an institution de novo? Vinod Aggarwal provides a framework[21], later co-opted by Jupille and Snidal, that prompts states to choose an existing institution to be the primary forum for cooperation to meet some goal, unless no existing institution fits the issue area that cooperation is meant to address[22]. States can either utilize these institutions as-is or modify them in such a way that they meet the criteria necessary to address the new problem[23]. When EC3 was first established within Europol, the specialization of Europol's functions to deal specifically with cybercrime could be seen as an example of institutional change – a pan-European institution that focused on cybercrime analysis and mitigation explicitly did not exist, but a pan-European institution that focused on crime in general did exist. Therefore, when the time came to establish an institution through which anti-cybercrime cooperation could be focused, it made sense to give an organization focused on cooperation against crime the responsibility to also facilitate cooperation against cybercrime. This is an example of nested substantive issue linkage, as cybercrime and crime at-large clearly display intellectual coherence. As an EU agency, states can see that greater cooperation against cybercrime within Europol's context also works toward the larger goal of stability within the EU[24]. Since substantive issue linkage also leads to the creation of a stable issue area and generally stable institutional arrangements[25], it is no surprise then that a formal institution was expanded as formal institutions are, by virtue of the overhead

required for their establishment, very stable relative to other arrangements. Such an increase in responsibilities also befits the rational institutional design conjecture that as the severity of the collective action problem increases, the issue scope of the organization increases[26]; given that cybercrime continues to grow in size and severity and every state remains susceptible to it, any organization assigned to support the mitigation of crime in general must increase its scope to include and specifically focus on cybercrime.

The aforementioned framework also suggests that Europol's use by states is dependent on whether it holds the status of a focal institution, an institution which is "widely accepted as a 'natural' forum for dealing with a particular cooperation problem"[27]. Decision costs and uncertainty about the world drive states to choose to utilize an existing institution and its current functions. As a state considers choosing from a group of institutions, augmenting a new institution, or creating a new institution, uncertainty increases with each of these choices, respectively. Therefore, the "use of a focal institution is usually the least costly resolution" and, as long as "actors are risk averse," they "promote safer strategies of use and selection"[28]. The importance of being recognized as a focal institution is echoed by Benoît Dupont, who finds in his network analysis on international cybercrime cooperation that some organizations attempt to outmuscle each other due to duplicate focuses, producing separate and competing networks of cooperation, with one network consisting of members exclusive from others[29]. As a collective action problem becomes more severe, institutions should attempt to be more inclusive in their membership[30]. Joining competing networks put states at a disadvantage as disparate membership across institutions weakens the ability of states to mitigate cybercriminal activity emanating from or in relation to a state within a competing institution, increasing the severity of the problem. Either most actors cooperate within one organization against cybercrime or they risk feeding the problem. Thus, a key assessment for the iterative cooperation hypothesis focuses on whether states consider Europol the focal institution for fighting cybercrime.

C. Material Conditions for Cybercrime Cooperation

In contrast to the idea that the perception of an institution drives states to cooperate within it, states could be driven by more material concerns, which would support the hypothesis that states cooperate with Europol to fight cybercrime to compensate for functional shortcomings that they cannot develop on their own immediately (cooperation by substitution). Bjorn Müller-Wille presents a framework that argues that "expanded co-operation within [Europol] would make sense if it added value to the fight against crime in general"[31]. Such cooperation must either produce something state agencies cannot produce alone, generate better intelligence than any agency could produce alone, or produce intelligence that state agencies cannot willingly or acceptably produce for political reasons[32]. Based on these criteria, a state should only be expected to cooperate within an international intelligence organization if there are tangible benefits, such as intelligence that is not reproducible by any single state's crime or intelligence agencies. Müller-Wille surmises that most of the information passing into Europol

was produced by state intelligence agencies and could theoretically be shared with other states without the use of Europol; hence, the advantages of expanded cooperation within Europol seem unclear[33]. States may also stray from cooperating within an organization due to the centralization of power in a specific region or institution[34]. Taking these concerns into perspective leads to the belief that states would not engage in the usage of an international institution in a context where national crime agency functions are duplicated. However, this would only be the case if Europol's singular function was to provide intelligence sharing. As stated before, Europol also provides training; technical support and expertise; and pivotally, partnerships with private firms through public-private partnerships. The potential to access these functions and partnerships drives states to cooperate within Europol against cybercrime.

Bendiek and Porter characterize EU cybersecurity policy as a multi-stakeholder structure, emphasizing public-private partnerships. The authors express that anti-cybercrime policy must focus on bringing governmental and nongovernmental actors together as partners. They argue that the current division of responsibilities among civil defense, military defense, and law enforcement sectors in regard to cybersecurity and, by extension, 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[35]. In practice, this informs the nature of cooperation between entities against cybercrime – interactions between states and state institutions arise as these institutions allow for cooperation among these stakeholders. These interactions progress toward formalized institutions – the authors specifically cite the example of Europol as a step toward international coordination against cybercrime[36]. Because private firms are now responsible for a large portion of public-facing critical infrastructure in Europe, including health care and energy, these firms are now targets for cybercriminals. Moreover, private firms such as information and communications technology (ICT) companies, including Microsoft and Symantec, have expertise and tools in fighting cybercrime that some states do not[37]. As such, their inclusion in cooperative networks is essential to organizations' attempts to foster effective anti-cybercrime cooperation[38].

There is some skepticism toward the effectiveness of public-private partnerships within the context of formalized agreements. Tatiana Tropina argues that states should continue to establish informal relationships with private firms, as the establishment of uniform compliance procedures could hinder the effectiveness of these private firms as partners against cybercrime[39]. Raphael Bossong and Ben Wagner disagree with Tropina and insist that formalized agreements support the effectiveness of public-private partnerships[40]. However, through the application of a cross-cutting analysis, they 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[41]. Whatever the effectiveness of public-private partnerships and whether firms believe it to be in their interest to cooperate with states, it is clear that states hold the potential of having private partners in fighting cybercrime in high regard, and therefore would be compelled to cooperate with an organization

through which those relationships could be exploited. Thus, states that do not have a high level of rapport with domestic ICT partners seek to augment their lack of relationships by cooperating within an institution such as Europol, which does have established partnerships with prominent, private ICT firms.

Domestically, a wide breadth and depth of nongovernmental partnerships and ICT sector size expansion require considerable time and investment to cultivate. Due to these costs, states could consider increases in partnerships and ICT sector size to be unachievable. Therefore, states seek access to institutions with a growing capability to fight cybercrime. This can be seen as another example of centralization. Previous work in rational institution design has shown that as uncertainty about the world increases, institutional centralization also increases[42]. As stated earlier in the discussion on the definition of cybercrime, all it takes is the use of a computer system in a malicious manner; anyone who can utilize a computer proficiently becomes theoretically capable of cybercriminal acts, which effectively increases uncertainty. Even if this capability is centralized within the institution itself and these capacities cannot be transferred over to the states, states can choose between having no capabilities and utilizing the institution's capabilities. Clearly the latter choice provides more utility. Thus, in establishing whether states cooperate within an institution with the intention of substituting an institution's capabilities for their own, it is first important to determine whether adequate domestic resources in the form of the technology sector and available partnerships exist.

D. Types of Anti-Cybercrime Cooperation

The significance of capacity building can be drawn from the choices states face when prompted with an institutional bargaining game. Aggarwal defines institutional bargaining games as bargaining games that consist of the types of goods that could provide some utility related to the issue area in question; the actors' individual situations, including their position in the international order, their domestic forces, and elite preferences within the state; and the presence or absence of institutions where bargaining would take place[43]. Institutional bargaining games result in different payoffs for different actors, which leads actors to attempt to strengthen their own positions[44]. When prompted with an institutional bargaining game, the actor (usually a state) can choose between three choices: they can attempt to alter the goods involved, they can alter their or their opponents' individual situations, or they can choose to alter an institution or create a new institution. This section focuses on the second option, where states attempt to alter their individual situation. In this context, the bargaining game is cybercrime mitigation, the institutional context is Europol, and the goods in question are Europol's operational support capabilities against cybercrime and its capacity building activities. States then cooperate within Europol in order to utilize the institution's capacity building abilities so that the state will eventually no longer need to utilize Europol's capabilities to fight cybercrime. Thus, this hypothesis supposes that states are cooperating to develop anti-cybercrime capabilities such that the states can eventually become self-reliant in the fight against cybercrime (cooperation

for self-reliance). What distinguishes cooperation for self-reliance from the type of cooperation discussed in the previous section (cooperation by substitution) is that the former focuses on states building capacities in the immediate term through support from the institution within which the state is cooperating, whereas the latter focuses on the use of the institution's capacities in lieu of the state's inability to develop similar capacities.

The framework for assessing cooperation for self-reliance draws primarily from Benoît Dupont's work on the international governance of cybercrime. Dupont maps interactions between states and organizations in the context of cybercrime to specific classifications[45]. He provides five categories of anti-cybercrime cooperation[46]:

- Capacity building;
- Information sharing;
- Regulatory and legal activities;
- Criminal investigations and intelligence collection; and
- Lobbying.

The overwhelming majority (74.5 percent) of initiatives Dupont includes in his dataset involves capacity building, while information/intelligence exchange characterizes 49 percent of these initiatives[47]. This finding also supports what some policymakers claim about cybercrime – capacity building remains the most important action in cybercrime mitigation[48]. However, Dupont professes that these connections do not show the intensity of the cooperation between states and nongovernmental organizations (NGOs) in fighting cybercrime or the intention behind their cooperation. He also goes on to state that data focused on methodologically similar, bilateral initiatives involving cooperation under Europol would produce significantly different results[49].

Since this paper focuses on cooperation against cybercrime within Europol, it is prudent to test Dupont's findings against this gap in the data. If states are driven to cooperate within an international organization primarily by a desire to develop their own abilities to fight cybercrime, then Europol's primary functions in facilitating intelligence sharing and providing operational coordination and support should not factor into cooperative actions against cybercrime heavily. In other words, a confirmation of the cooperation for the self-reliance hypothesis suggests that states want and generally seek to go it alone in the fight against cybercrime, and most cooperate within institutions in order to reach a point of independence. If this were to occur, they would no longer be affected by the threat of cybercrime as they were before they began cooperating within the institution. In the language of institutional bargaining games, at the point of self-reliance, states successfully change their individual situation and, therefore, their payoff structure within the game. While this assertion runs contradictory to the operational nature of Europol's activities, it is nevertheless important to assess this hypothesis in order to ascertain whether the desire to build capabilities effectively drives state police agencies to cooperate within institutions against cybercrime.

III. METHODOLOGY

This paper tracks a different variable or set of variables for each hypothesis. For the first hypothesis, iterative cooperation, I utilize interview responses and policy data to show whether Europol is seen as a focal institution. For the second hypothesis, cooperation by substitution, I utilize a combination of survey data and interviews to measure how much interaction states have with domestic ICT partners. I also measure the ICT sector size in each state by measuring ICT employment as a percentage of total employment within each Europol member state and compare each country's differential to the mean percentage in order to ascertain the size of each state's ICT sector relative to a central tendency. A percentage of ICT employment is utilized to estimate ICT sector size as opposed to absolute employment numbers in order to normalize the size of each state's ICT sector relative to other member states; utilizing absolute employment numbers results in misleading data due to the population differentials across states. These two variables measure both the reality of interactions and the potential for partnerships that state law enforcement agencies can have with private firms, and therefore characterize whether a state needs to act through Europol to interact with private firms and NGOs or seek out foreign technical expertise. Finally, for the third hypothesis, cooperation for self-reliance, I measure several variables, including the amount of funding a state police agency received and the amount of training requested from Europol in order to capture the number of interactions states had with Europol that can be categorized as capacity building. Also included is data collected from interviews which categorize the frequency and importance of capacity building activities (namely, training and funding) from the point-of-view of Europol officials.

The primary limiting factor of this methodology is the lack of data available from state law enforcement agencies on their activities within Europol. Of the 28 member states that were asked to participate in the qualitative survey, only one (the United Kingdom) gave responses. Of the 28 member states that were asked to participate in the quantitative survey, only one (Denmark) responded. The United Kingdom and Germany both purported to not have the necessary information to answer the quantitative questionnaire. This makes it incredibly difficult to draw strict conclusions from these findings as the lack of data limits the variance required to validate the results. Nevertheless, even with the lack of data, valuable insights can still be gleaned from the results collected.

IV. RESULTS

The following section discusses findings from interviews conducted with Europol's Head of Strategy, Philipp Amann; an interview conducted with the United Kingdom's National Cyber Crime Unit (NCCU); and survey data collected from a questionnaire given to Denmark's National Cybercrime Center (NC3). The survey 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; frequency of interac-

tions with domestic and international, nongovernmental technology partners; and one free-response question focusing on agencies' capabilities in comparison to Europol's. The evidence also includes data collected from EU policy documents.

A. Identifying Europol as a Focal Institution

To measure whether Europol is seen as a focal institution, a combination of data was collected from policy analyses, interviews, and survey data. The EU's overall cybersecurity strategy cites Europol "as the European focal point in the fight against cybercrime"[50]. The strategy explicitly assigns the responsibility of facilitating anti-cybercrime cooperation among states and cooperation between states and private or nongovernmental stakeholders to Europol [51]. These statements leave no ambiguity that Europol carries the distinction of being considered a focal institution, at least from the point-of-view of the EU itself. By extension, Europol is undoubtedly seen as a focal institution against cybercrime from the point-of-view of many policymakers.

From the perspective of the institution, Europol does not directly inform a member state that its protections against cybercrime require improvement unless the state in question asked Europol for an assessment[52]. Member states participate, including the sharing of open-source reports, malware, and other forms of data, on a voluntary basis[53]. Should a member state choose not to share its intelligence, Europol cannot force a state to share that intelligence. As for reasons why a member state would not cooperate with Europol, member state law enforcement agencies are often either unaware of or ignore the resources Europol can provide[54]. 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[55]. Europol officials see this as law enforcement agencies across member states being unaware of what Europol can provide those agencies, and therefore do not reach out to the institutions as much as they could[56]. Survey data collected from the Danish NC3 reinforces this supposition; the center remarked that only up to a fifth of anti-cybercrime operations in the most recent year involved direct operational support from Europol[57].

While the perceived lack of use by state police agencies suggests that states do not view Europol as a focal institution for cybercrime mitigation, further elaboration about the nature of the problem of cybercrime actually suggests that Europol is viewed as a focal institution for cybercrime mitigation by member states. In a comment at the end of the survey, NC3 stated that "the resources and capability of the member states...holds [sic] back the common process. Cyber [crime] has to be prevented and fought from an international perspective"[58].Furthermore, rather than pursuing policy-based prescriptions to bring agencies into the fold, Amann suggests that Europol needs to do a better job of advertising and reaching out to law enforcement agencies[59]. The choice to attribute the perception that Europol lacks usefulness to lack of outreach rather than tying it to a need for hierarchical structure indicates either an unwillingness to establish a more hierarchical structure or a belief that a more hierarchical structure is unnecessary. Even with the voluntary nature of state crime agencies' relationship with the in-

stitution, Amann remarked that the member states do utilize Europol effectively[60]. This statement, coupled with the statement from NC3 regarding the need to fight cybercrime from an international perspective, leads to the conclusion that the international nature of cybercrime gives states the impetus to place a premium on platforms for international anti-cybercrime operations, such as Europol.

B. Measuring Agency Use of Europol to Substitute Capacities

To assess whether Europol is used by states to substitute a lack of capability, a combination of interviews, survey data, and domestic ICT employment sector size data is utilized to determine whether a state's law enforcement agency perceives its available capabilities to be up to par with Europol's and whether the potential for increased partnership and capabilities exists. A measurement of these variables illustrates whether states perceive that Europol's available capabilities and partnerships within the context of mitigating cybercrime are more valuable than the state's domestic capabilities and partnerships.

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[61]. 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, Europol officials, and third parties with cooperation agreements with Europol can communicate with and disseminate intelligence to other partners or to Europol itself[62]. Europol also conducts malicious software (malware) analysis through the Europol Malware Analysis System (EMAS) [63]. 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 its investigation or active operation. Member states have access to the Digital Forensics and Mobile Laboratory, which mines data from hard drives and mobile phones, and Europol's password decryption platform[64]. Lastly, Europol interfaces with outside partners, including Interpol and third-party states, as well as nongovernmental partners, including private firms, accepting information from them, including internet protocol (IP) addresses, and consulting nongovernmental partners in an advisory capacity[65]. When asked whether NC3 could claim equivalent anti-cybercrime capabilities to those of Europol, the agency responded, "No"[66]. The NCCU stated that capabilities across member states varied widely and, at times, bilateral interactions with partners with similar capabilities resulted in more fruitful interactions; however, bilateral relationships lacked the ability to pool resources from other member states or construct the "big picture" pertaining to the issue at hand[67].

Europol also maintains relationships with public-private partners for operational and advisory purposes. Private firms and NGOs provide Europol with intelligence, including IP addresses

of potentially compromised or potentially suspicious computers[68]. Private firms and NGOs are also utilized in an advisory capacity through membership with an advisory board[69]. Most member states are thought to hold their own relationships and partnerships with private firms and NGOs, but these are not tracked by Europol. Thus, the relationship between member states and EC3 is not at all hierarchical, despite the fact that institutional policy drives the direction of the relationship[70]. The NCCU remarked that business and reputational costs often stand in the way of forming partnerships with private firms. However, private firms seem to be willing to share more information on some types of attacks, such as DDoS attacks, due to the lower reputational risks associated with them in comparison to attacks that disclose user data[71].

While all of this illustrates that Europol has considerable capabilities of which member states can take advantage and that these capabilities encourage states to engage in cooperation within Europol against cybercrime, survey data illustrates that member states might already have comparable capabilities. Table 1 shows the results of a survey answered by NC3 with respect to the proportion of interactions the agency has with ICT partners both through and outside of Europol as well as the Danish ICT sector size compared to the average Europol member state sector size.

Danish Cybercrime Interactions*	
Category	**Percentage**
Private sector partners who also have partnerships with Europol	1-20%
Private technology partners through Europol	1-20%
Private sector partners that are also domestic partners	41-60%
EU state police agencies that occurred through Europol	21-40%
2016 national ICT sector employment percentage compared with average Europol member state 2016 ICT sector employment (SD = 1.2)	+0.6%

*All from 2017 unless otherwise noted

TABLE 1

These results indicate that the overwhelming majority of cybercrime operations in the Danish case do not require direct operational involvement from Europol. Denmark clearly has above-average domestic technology partnerships and available domestic technological prowess; most of NC3's interactions with private partners occur outside of Europol, and around half of these interactions are with domestic, private firms, which eliminates the need to interact with them through an international organization in the first place by virtue of their domesticity. Most interactions with other Europol member states' police agencies occurs outside of the organization. Even the Danish ICT sector size is one-half standard deviation above the average Europol-member ICT sector size – a medium-sized difference from the average Europol member state [72]. These results also indicate that there exists a potential for greater utilization of domestic partnerships and technical expertise in comparison with other member states.

C. Measuring Agency Use of Europol to Build Capacity

To measure the frequency and importance of capacity building activities to Europol, it is important to first know Europol's available capacity building activities. The dissemination of training, funding, and technical tools can be considered a capacity building activity. Much of the institution's educational outreach and operational support focuses on establishing a baseline level of expertise among member states to ensure effective cross-border cooperation[73]. Europol also provides funding to member state agencies to implement policy objectives; this funding can also be used to implement joint, international projects proposed by member state agencies[74]. Free anti-cybercrime tools, such as forensic analysis tools developed through the FREETOOL project, are also provided to member states[75]. Training to utilize these tools is provided through Europol.

Europol officials find that capacity building activities hold a relatively low frequency and importance in comparison to other Europol functions. Amann ranks the following cooperative actions against cybercrime in order of importance 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.

With these results, Dupont's finding that capacity building makes up the overwhelming plurality of cooperative interactions against cybercrime[76] comes under scrutiny. This complicates the cooperation for self-reliance hypothesis. If capacity building only includes education and prevention outreach, then when examining the metrics of importance and frequency, capacity building is seen as both least important and least frequent. If operational support (in particular, intelligence sharing and analysis) can be categorized under capacity building, then capacity building becomes both most important and most frequent[77]. However, operational support does not include common actions associated with capacity building, such as education. Admittedly, Amann emphasized that the differences in importance among these three actions are minimal, the relationships among the three are close, and each type of cooperation is often tied to another type of cooperation[78]; the NCCU also emphasized this[79]. Sometimes officers are sent from member state crime agencies to work on specific cases if necessary[80]. There exist ample opportunities for states to request operational support, although intelligence sharing does make up the bulk of the day-to-day work. However, capacity building activities seem to be in sparse supply.

Results from the questionnaire given to member-state police agencies also seem to indicate that capacity building does not characterize cooperation within the organization. Survey responses from NC3 with respect to the agency's interactions with Europol strictly pertaining to capacity building activities show that the agency does not utilize Europol very much to build

capacity: the agency requested no funding and only two instances of training in the most recent fiscal year.

These figures correspond accordingly with the statements from Europol officials on the frequency of cybercrime-related training. It must be noted that Europol does not provide many instances of training per year[81] and, therefore, numbers pertaining to training may be relatively low no matter what; however, the amount of requested funding is telling. Funding can be used to develop new technologies, hire new staff, provide training, and invest in new projects, all of which are clearly capacity building activities. Given that the previous sections have illustrated that NC3 finds cooperation with Europol incredibly important in fighting cybercrime, the fact that the agency requested no funding in the 2017 fiscal year shows that capacity building must not matter much in the calculus of that state's national law enforcement agency.

V. ANALYZING CONDITIONS FOR COOPERATION

The first hypothesis is tested by demonstrating whether states viewed Europol as a focal institution in cybercrime mitigation; if states considered Europol a focal institution in cybercrime mitigation, then, by Aggarwal's framework, iterative cooperation drives cooperation within Europol against cybercrime. When the decision was made to expand into the realm of cybercrime, Europol's preexisting structure may have given it the ability to establish its capabilities and reputation to a point that supersedes the capabilities and reputation of member-state police agencies. 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[82]. The establishment of the organization predates many of the member-state cybercrime agencies, only some of which, such as the Greek agency, predate the establishment of Europol[83].

While Europol's cybercrime center postdates many of the member state agencies' cybercrime centers, states do not seem to feel the need to deviate from Europol's preestablished 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, states require less overhead to be convinced to engage in new forms of cooperation. The remark made by the NC3 indicates that Europol's known reputation and ability entice states to approach the organization with some degree of confidence. This lines up with the perception that Europol is a "focal" institution against cybercrime.

In testing the second hypothesis, ICT employment data for each state was collected alongside survey data that measured a state police agency's involvement with domestic ICT partners (table 1). If a state's ICT sector size was small compared to the average Europol member state ICT sector size or the state police agency had weak involvement with ICT private firms and NGOs, then that state should be more driven to cooperate within Europol. When combining the ICT employment percentages compared to the average EU employment percentage, the Danish response to the survey was illuminating. According to the results, Denmark had above-average

ICT employment as a percentage of total employment when compared to other Europol member states[84]. Only up to 20 percent of NC3's interactions with nongovernmental technology partners occur through Europol[85]. Around half of the agency's interactions with nongovernmental technology partners occur domestically; these do not require interaction with Europol to access[86]. Prima facie, all of these data points suggest that such a state should be less dependent on Europol's potential opportunities for access. Nevertheless, it seems that even a relatively small need to fight potential cybercrime threats internationally results in a willingness to engage in cooperation within the institution, regardless of the number of problems those activities can solve. While Denmark did not have a small ICT sector size relative to the average Europol member state sector size and had frequent interactions with technology partners outside of Europol, this did not change NC3's professed willingness to cooperate within the institution.

Furthermore, NC3's perception that its capabilities do not match Europol's and the survey results are at odds. It seems clear from the data that the idea that Europol needs to provide most of the necessary partnerships to member states to encourage cooperation does not hold water. Again, this might point to states' and state police agencies' views on the nature of the problem of cybercrime – this is an issue area for which agencies perceive there is no limit to increased support and expertise; however, this increased support and expertise do not necessarily amount to the wholesale substitution of Europol's cybercrime mitigation capabilities with domestic ones. Therefore, while it may allow states to increase their abilities to fight cybercrime, cooperation in the name of substituting capabilities only provides marginal improvement in some cases and serves more as a secondary driver toward state involvement within Europol than as a primary one. This leads to the conclusion that an intrinsic property of the problem, the international nature of cybercrime, serves as a primary motivator behind states' willingness to cooperate within an institution to fight cybercrime; in addition, other potential avenues for mitigation, specifically domestic avenues, are not enough to make a state's police agency feel secure.

Testing the third hypothesis involves identifying whether international cooperation within Europol focuses on capacity building; if a large proportion of cooperation does focus on capacity building, then states are driven to cooperate within the institution to build a sustainable, domestic, anti-cybercrime apparatus. As noted from the interview with Amann, each cooperative action is classified according to Dupont's categories[87] to ascertain whether international cooperation against cybercrime focuses on capacity building.

Table 2 maps the categories Dupont presents in his work to the types of operations available through Europol. Clearly, these operations do not cleanly fall into the different categories. For example, as an open-source (free-to-use) project, the development of the FREETOOL project can be considered an instance of 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 intelligence concerning malware. Furthermore, 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[88]. This overlap makes it difficult to provide a discrete category for each type of cooperation. Given that intelligence sharing makes up most of Europol's day-to-day work, it seems reasonable to conclude that the exchange of information trumps all of the other categories in frequency. 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. Therefore, if capacity building only encompasses funding, education, and capability development, then capacity building comes in third behind information exchange and law enforcement operations, respectively. Since capacity building only makes up a relatively small amount of cooperative measures that occur within Europol, cooperation for self-reliance seems to be a weak driver in encouraging states to cooperate within Europol against cybercrime.

Europol Classification of Anti-Cybercrime Activities	
Category of Action	**Action/Operation**
Capacity building	• Training 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

Based on these findings, it is reasonable to posit that while capacity building does play an important role in anti-cybercrime cooperation, states may not focus on it if an organization is capable of facilitating more direct means of engaging potential threats. NC3's survey responses (table 1) 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 percent of interactions with other EU member-state crime agencies required interaction with the agency through Europol, and up to 20 percent of anti-cybercrime operations required the direct involvement of Europol[89]. Despite neither of these interactions making up the majority of Europol's types of operations, they still occur at regular enough frequency to be considered the primary work of Europol. Based on this evidence, the desire to build capacity only has a minimal-to-moderate effect on states' cooperation within an institution to fight cybercrime.

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 have different cultural attitudes toward policing that affect their willingness to cooperate internationally with other law enforcement agencies or with nongovernmental partners. He brought up the example of the Netherlands, where many of the banks have close partnerships with anti-cybercrime initiatives and policing agencies. In addition, Dutch banks interface with anti-crime task forces to disseminate information to other banks and law enforcement representatives in the same room[90]. These partnerships may 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 variance in legal frameworks across these countries also factors into whether these types of cooperative relationships are possible. The NCCU noted that this is a large challenge in regard to working within the institution[91].

Another confounding variable that was brought up in the interview was the size of countries' bureaucracies. Citing Estonia, Amann noted that the country itself is small in population and does not have the same degree of bureaucratic complexity as larger member states, such as Germany and France. The lack of bureaucratic complexity leads to a reduction in formal structures in comparison with larger countries, leading to a smaller amount of people taking on a larger amount of responsibilities. This increases the responsiveness between government officials of smaller countries and Europol at the cost of higher barriers to establishing relationships with Europol when government officials first take office[92]. In contrast, the Netherlands contains many formalized structures for partnerships with Europol, which creates a different approach to and platform for cooperation. Bureaucratic turnover also creates problems. The constant turnover of senior management in Europol member states leads to a lack of institutional memory among government staff and policymakers[93]. This turnover may result in a new staff that does not know how to harness Europol resources effectively and efficiently.

VI. CONCLUDING THOUGHTS AND NEXT STEPS

Given the evidence presented in this piece, the strongest driver for participation in Europol is iterative cooperation. 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, even if states had already established a cybercrime unit that predated EC3. Contributing to this willingness to cooperate also seems inherent to the problem of cybercrime; that is, effective mitigation must be international in scope.

Cooperation by substitution and cooperation for self-reliance, on the other hand, are weaker drivers. As seen in the case of Denmark, an above-average ICT sector size in terms of the percentage of employment does not lessen the value that the state's cybercrime unit places on Europol's utility in fighting cybercrime. Observations on the types of support that Europol gives also seem to focus readily on operational support and information exchange, effectively supplanting capacity building as the most frequent and important type of interaction. Again, it seems that reputation and ability play directly into how states act within Europol. The

organization's structure and services lend themselves to direct support to 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.

More data from other Europol member state police agencies must be taken into account before drawing further policy implications. The current version of this project only observes two states, which both have a higher-than-average technology sector size in terms of ICT employment percentage[94]. The next step would be to see whether data obtained from member states with a lower-than-average technology sector size would provide similar results to those of the states examined so far. Furthermore, there exist 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 whether the organization is seen as a focal institution due to a lack of available competition. The lack of a competing agency without Europol's reputation cannot be tracked to measure its comparative utilization, weakening the ability to establish a direct causal link between Europol's existence and its image as a "focal" institution.

Nevertheless, the preconditions of reputation and known competence must be taken into account as important considerations should IGOs and NGOs want to encourage international members to cooperate, whether addressing cybercrime or some other matter of international security. In his interview, Amann summed up the biggest factor in one word: "trust." This is not just trust in one's partners, however; it is trust that cooperation leads to successful operations. This indicates that the overhead necessary to convince states to cooperate is considerable, but, once that overhead has been established, states no longer need much convincing.

ACKNOWLEDGEMENTS

I would like to thank Vinod Aggarwal, Amy Gurowitz, and Andrew Reddie of the University of California, Berkeley, for advising me throughout this project. I would especially like to thank Andrew, whose continued support over the past two years led me to formulating and pursuing this topic in the first place. I would like to thank Philipp Amann at Europol and Paul Timmers for speaking with me as I wandered through Europe attempting to obtain data on cybercrime cooperation. I would also like to thank Tobias Hofmann at the University of Utah, whose feedback alongside Andrew's led me toward the institutional design frameworks. Finally, I would like to thank the Center for Long-Term Cybersecurity at the University of California, Berkeley, for allowing me to utilize its space while working on this project.

NOTES

1. Nick Eubanks, "The True Cost of Cybercrime for Businesses," Forbes (blog), July 13, 2017, https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/.
2. European Parliament, "REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016," EUR-Lex - Access to European Union Law, May 5, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0794&from=EN.
3. Philipp Amann, Interview with Philipp Amann, Head of Strategy, European Cybercrime Center, In-Person, January 8, 2018.
4. "Operational Agreements," Europol, accessed April 29, 2018, https://www.europol.europa.eu/partners-agreements/operational-agreements.
5. Denmark was the last state to re-join Europol after Danish voters rejected a 2015 referendum that would have allowed Denmark to opt-in on EU home and justice matters on a case-by-case basis. A separate agreement was eventually struck between the EU and Denmark that allowed continued use of Europol in 2017.
6. "EU Policy Cycle - EMPACT | Organised Crime | Europol," accessed April 29, 2018, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.
7. NCCU Research, Interview with United Kingdom National Cyber Crime Unit, Text, February 21, 2018.
8. "European Cybercrime Centre - EC3," Europol, accessed April 29, 2018, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
9. NCCU Research.
10. Amann.
11. "Symantec and Europol Strengthen Cooperation in Joint Fight against Cybercrime | Europol," accessed April 29, 2018, https://www.europol.europa.eu/newsroom/news/symantec-and-europol-strengthen-cooperation-in-joint-fight-against-cybercrime.
12]. Elaine Fahey, "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 24, 2014), https://papers.ssrn.com/abstract=2384491.
13. Ibid.
14. Ibid.
15. "Internet Organised Crime Threat Assessment (IOCTA) 2017."
16. Felicity Vabulas and Duncan Snidal, "Organization without Delegation: Informal Intergovernmental Organizations (IIGOs) and the Spectrum of Intergovernmental Arrangements," The Review of International Organizations 8, no. 2 (June 1, 2013): 193–220, https://doi.org/10.1007/s11558-012-9161-x.
17. Kenneth W. Abbott and Duncan Snidal, "Why States Act through Formal International Organizations," The Journal of Conflict Resolution 42, no. 1 (1998): 3–32.
18. Barbara Koremenos, Charles Lipson, and Duncan Snidal, The Rational Design of International Institutions (Cambridge, UNITED KINGDOM: Cambridge University Press, 2003), http://ebookcentral.proquest.com/lib/berkeley-ebooks/detail.action?docID=255150.
19. Abbott and Snidal.
20. Ibid.
21. Vinod K. Aggarwal, Institutional Designs for a Complex World: Bargaining, Linkages, and Nesting (Cornell University Press, 1998).
22. Joseph Jupille and Duncan Snidal, "The Choice of International Institutions: Cooperation, Alternatives and Strategies," SSRN Electronic Journal, 2006, https://doi.org/10.2139/ssrn.1008945.
23. Ibid.
24. Aggarwal.
25. Ibid.
26. Barbara Koremenos, Charles Lipson, and Duncan Snidal, The Rational Design of International Institutions (Cambridge, United Kingdom: Cambridge University Press, 2003).
27. Jupille and Snidal, "The Choice of International Institutions."
28. Ibid. See also Koremenos, Lipson, and Snidal.

NOTES

29. Benoît Dupont, "La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale," Cultures & Conflits, no. 102 (August 8, 2016): 95–120, https://doi.org/10.4000/conflits.19292.
30. Koremenos, Lipson, and Snidal.
31. Björn Müller-Wille, "The Effect of International Terrorism on EU Intelligence Co-Operation," JCMS: Journal of Common Market Studies 46, no. 1 (January 1, 2008): 49–73, https://doi.org/10.1111/j.1468-5965.2007.00767.x.
32. Ibid.
33. Ibid.
34. Zahid Jamil, "Global Fight against Cybercrime: Undoing the Paralysis," Georgetown Journal of International Affairs, 2012, 109–20.
35. Ibid.
36. Ibid.
37. Dupont.
38. Bendiek and Porter.
39. Tatiana Tropina, "Public–Private Collaboration: Cybercrime, Cybersecurity and National Security," in Self- and Co-Regulation in Cybercrime, Cybersecurity and National Security, SpringerBriefs in Cybersecurity (Springer, Cham, 2015), 1–41, https://doi.org/10.1007/978-3-319-16447-2_1.
40. Raphael Bossong and Ben Wagner, "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU," Crime, Law and Social Change 67, no. 3 (April 1, 2017): 265–88, https://doi.org/10.1007/s10611-016-9653-3.
41. Ibid.
42. Koremenos, Lipson, and Snidal.
43. Aggarwal.
44. Ibid.
45. Dupont.
46. Ibid.
47. Ibid.
48. Heli Tiirmaa-Klaar et al., "Botnets, Cybercrime and National Security," in Botnets, SpringerBriefs in Cybersecurity (Springer, London, 2013), 1–40, https://doi.org/10.1007/978-1-4471-5216-3_1.
49. Dupont.
50. European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," European External Action Service, July 7, 2013, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
51. Ibid.
52. Amann.
53. NCCU Research.
54. Amann.
55. Ibid.
56. Ibid.
57. NC3, Interview with Danish National Police Cyber Crime Center, Text, March 16, 2018, 3.
58. Ibid.
59. Amann.
60. Ibid.
61. James Igoe Walsh, The International Politics of Intelligence Sharing (Columbia University Press, 2010), https://doi.org/10.7312/wals15410.
62. "Secure Information Exchange Network Application (SIENA) | Activities & Services | Services & Support | Information Exchange | Europol," accessed April 29, 2018, https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena.
63. Amann.

NOTES

64. NCCU Research.
65. Amann.
66. NC3.
67. NCCU Research.
68. Amann.
69. Ibid.
70. Ibid.
71. NCCU Research.
72. Jimmie Leppink, Patricia O'Sullivan, and Kal Winston, "Effect Size – Large, Medium, and Small," Perspectives on Medical Education 5, no. 6 (December 2016): 347–49, https://doi.org/10.1007/s40037-016-0308-y.
73. Amann.
74. Ibid.
75. "FREETOOL v2.0 | UCD Centre for Cybersecurity & Cybercrime Investigation," accessed April 29, 2018, http://www.ucd.ie/cci/projects/current_projects/freetool2.html.
76. Dupont.
77. Amann.
78. Ibid.
79. NCCU Research.
80. Amann.
81. Ibid.
82. European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace."
83. Philip Chrysopoulos, "Greek Police Transfers Cyber Crime Unit Chief, Then Repeals Decision, Then Transfers Him | GreekReporter.Com," February 18, 2016, http://greece.greekreporter.com/2016/02/18/greek-police-transfers-cyber-crime-unit-chief-then-repeals-decision-for-now/.
84. European Commission, "Eurostat," Eurostat: Your key to European statistics, August 11, 2016, http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables.
85. NC3.
86. Ibid.
87. Dupont.
88. Amann.
89. NC3.
90. Amann.
91. NCCU Research.
92. Amann.
93. NCCU Research.
94. European Commission, "Eurostat."