The FATF as a Model for Internet Governance

Kevin P. Newmeyer
Assistant Professor
Center for Hemispheric Defense Studies
Washington, DC
kevin.newmeyer2@ndu.edu

Abstract— **To date, traditional diplomatic instruments and structures have only been marginally effective in combating cybersecurity risks. Perhaps it is time to use a model that has been effective in another challenging international arena, money laundering. The Financial Action Task Force (FATF), which started as an effort among the economic leaders in the world, uses an intergovernmental policy group to build political will to counter a network threat. With its best practices, regional sub-groups, and threat of blacklisting, it is effective in bringing pressure to bear on recalcitrant nations. A FATF style cyber security body offers a means to improve the global governance regime for the Internet by leveraging the will of interested governments. This paper offers an outline of how the FATF model could be applied to the Internet, and thereby improve governance and security.**

Keywords-component; cybersecurity, governance;, international; security; cooperation

I. INTRODUCTION

Threats to computer systems, networks, and even personal financial data exploded over the past several years. The threat has changed from the random teenager looking for excitement by trying to penetrate a university's network to sophisticated criminal enterprises capable of stealing or extorting millions of dollars. The advent of the Stuxnet virus and the Aurora attacks of 2010 realized the potential for nation state involvement in cyber attacks at a new level [1]. Malware continues to increase with one vendor reporting an average of 73, 190 new samples of malware discovered on a daily basis [2]. A study published by the Internet security firm McAfee in early 2009 put the global price tag for cybercrime at one trillion dollars when counting the loss of intellectual property and the direct costs to cleaning up after breaches [3].

Currently at the international level, there are few tools or mechanisms to improve cybersecurity in the growing electronic global commons. The Council of Europe Convention on Cybercrime [4] currently stands as the primary international treaty with cyber implications. The Convention is useful for defining and criminalizing many hostile cyber activities, but it retains a focus on criminal activity. Additionally, while there is broad European accession to the treaty, the United States is the only non-European country to have ratified the treaty whereas significant countries such as Russia and China have not even signed the Convention [4]. This significantly weakens the usefulness of the treaty as a global instrument. In a paper prepared for the Twelfth United Nations Congress on Crime Prevention and Justice, Judge Stein Schjolberg of Norway commented that global deterrence against cyberthreats may best be achieved with a United Nations convention [5]. The treaty proposal however was met with limited support. Issues include national sovereignty, privacy concerns, and the length of time required to negotiate and ratify a treaty when the Council of Europe Convention is already in place [6]. Treaties are also legally binding instruments in international and domestic law. They represent the highest level of agreement between states on the manner to resolve common issues and disputes and therefore are difficult to achieve in many cases.

An alternative, less formal but highly effective model of international cooperation already exists that may be applicable to the cybersecurity problem. The Financial Action Task Force (FATF) was created in 1989 to counter money laundering with a structure that is flexible and adaptable to address emerging challenges such as terrorist financing and proliferation financing [7, 8]. This paper will discuss the organization and operation of the FATF in its role as an international organization combating a security threat and show how a similar organization might be effective in improving global cybersecurity governance.

II. THE FATF MODEL

A. *Description of the FATF*

The Financial Action Task Force consists of a small secretariat based in Paris at the Organization for Economic Cooperation and Development (OECD) and representative from over 30 member states (8). It operates under a ministerial mandate to establish international standards to combat terrorist financing and money laundering (8). The standards are not binding legal instruments as in a treaty but represent the consensus opinion of the FATF on what are the best practices to be adhered to by member states and other actors in the international financial system. The standards are in fact referred to as "recommendations". Additionally, the

978-0-615-51608-0/11 ©2011 EWI

FATF conducts periodic reviews and assessments of its members, researches and publishes typologies on financial crimes, and assesses and responds to new risk areas such as proliferation financing [8].

While the core FATF is focused on the major industrial economies, it developed a system of regional subordinate organizations that allow for focus on smaller economies in geographical groupings. The FATF establishes the policies and recommendations which are then passed on to the FATF-style regional bodies (FSRBs). The FSRBs provide a forum and representation for smaller countries and jurisdictions. They provide greater understanding for smaller economies and regional cultural differences while maintaining the ministerial level commitment to adherence to international standards and mutual assessments of effectiveness. The FRSBs are represented in the FATF deliberations as blocs with voting privileges. In total, more than 180 jurisdictions are members of the FATF and/or a FRSB [8]. The United Nations, World Bank, International Monetary Fund, and several regional organizations are also participants or official observers in the FATF and FSRBs.

B. *Reasons behind the effectiveness of FATF*

The key processes of the FATF are the establishment of global standards and the mutual evaluation process to ensure that standards are met. The FATF membership is limited and selective. Its membership however includes the bulk of the world's financial activity [9].

The FATF focuses on two primary goals: global coverage and global compliance [10]. By getting as many countries as possible to participate in the AML/CFT regime established by the FATF recommendations, the FATF leveraged its regional associates. The organization now contains the vast majority of the world's economic actors and can marginalize the illicit actors. The global compliance focus is perhaps one of the greatest achievements of the FATF. The organization is not afraid to use a name and shame process, its non-compliant countries and territories (NCCT) list to indicate and isolate threats to the global system [9]. Former U.S. Deputy National Security Advisor for Combating Terrorism, Juan Zarate highlighted the effectiveness of using market forces to achieve compliance [7]. The NCCT list identified to the private sector the increased risk of doing business with entities in the non-compliant jurisdiction. It thereby provided the private sector the power to isolate potential threats to their business based on objective criteria. If a country did not choose to follow and enforce the rules of the game, it risked being isolated from global financial markets and the negative impact to the country's economy. The NCCT process was replaced in 2007 with the International Cooperation Review Group (ICRG) and a series of public statements on high risk countries [11]. The ICRG process continued the naming and shaming tradition.

The FATF process is not only a stick to the non-compliant. It offers economic benefits to states that participate. In addition to direct assistance provided by FATF members and the FSRBs for training and compliance improvement, there are indirect financial incentives. Compliance with the FATF recommendations increases the transparency of a country's financial and legal systems [7, 8, 9]. Higher compliance reduces corruption and lowers the risk to international financial partners which in turn allows for better terms [10]. Both result in greater value to governments and citizens.

III. Cybersecurity Application of a FATF Model

A. *Basis for a FATF Model*

The internet is now a global network operating under a collection of national rules in different countries but without a formal governance structure over its global commons. International accords are somewhat limited and questions of sovereignty and even borders in a cyber world remain the focus of debate. While several models for governance have been put forward by academics, none have resonated fully on a global basis. In an age where money flows across borders as an electronic message and paper currency is being replaced ever more often by electronic substitutes, the FATF model proved to be effective in at least raising the bar to illicit activity. It required countries to [8]:

- Investigate and prosecute money laundering and financial crimes
- Deny criminals access to their illegal gains
- Place a burden on financial system service providers to implement controls for due diligence, suspicious activity reporting, and record keeping
- Implement oversight mechanisms to ensure susceptible businesses and professions comply
- Improve transparency for legal persons to ensure accurate ownership information is available to authorities
- Establish international cooperation and information sharing mechanisms

In essence, it established a minimum set of standards and a forum for cooperation and coordination at an international level. The model was effective because it could be used to isolate jurisdictions from the global financial system if they did not follow the rules [7].

The global internet space resembles the global financial market in many ways. The financial network is in reality a subset of the internet with applications for trading, commerce, trade payments, and money movement. Regulations are largely national, and control is a function of territorial jurisdictions. The FATF provided the minimum rules of the game with enforcement left to local actors under an international framework. The effect of the internet on global financial regulation has been an issue for many years [12]. In 1996, Commodity Futures Trading Commission Commissioner Tull called for internet regulators to be as flexible as the medium itself [12] at a time when there were 68 million users and half a million websites. Now there are nearly 2 billion users globally [13] and more than 255 million websites as of December 2010 [14]. The numbers continue to grow. Our ability to secure cyberspace has not kept pace and the Internet is now the locus of crime on a massive scale. The FATF made it harder for criminals to abuse the financial network; a similar construct may work for the Internet. The FATF gained the respect of the international community [8]; such respect is also needed for an internet governance body.

B. A Model for Security Governance on the Internet

Like the financial network, cyberspace is open to abuse by criminal elements. Also in parallel to the financial network, criminals require a point of entry into the internet. A viable system of governance requires transparency, international coordination, reporting requirements, and a mechanism to compel compliance with the governance framework. For the internet to continue to grow, trust must exist in on line transactions and activities [15]. A FATF modeled internet governance system addresses these concerns.

The initiative should be sponsored and implemented by the G-20. This group comprises the bulk of the world's population, capital, and internet users. Much as the FATF grew from a G-7 initiative in 1989 to be a global organization with more than 180 associated countries, the G-20 could provide a nucleus of important players to create an internet governance forum focused on increasing the security of the system for not only nation states but individuals as well. A G-20 based structure allows interested parties to make ministerial level commitments in a rapid and open format. It must include the principal users and consumers of the internet as well as the countries that provide the bulk of the physical infrastructure that carries internet traffic. This body would be tasked with developing a list of best practices and security requirements that members must adopt similar to the FATF money laundering and terrorist financing recommendations. This would be an inter-governmental body with representation from multiple sectors of government. It should include at a minimum foreign affairs, justice, defense, economic, and civil protection/homeland security ministries at the discretion of the participating countries.

Additional members or observers to the core group must include the private sector. The vast bulk of the service providers of ICT, both hardware and software, are in the private sector. Economic and business interests are now intricately tied to cyber. Their expertise and cooperation is needed to increase security and consumer confidence [15]. The private sector already participates in activities of the International Telecommunications Union, the United Nations body with the lead on ICT issues [15]. The Conficker Working Group demonstrated the effectiveness of public-private cooperation in addressing internet based threats [16]. That group brought together experts from several sectors to combat an advanced botnet threat. They demonstrated flexibility and adaptability to counter a challenging threat. The lessons learned from this process would be extremely valuable to a successor organization.

Existing global bodies, particularly from the UN organizations, should also be granted observer status. The knowledge base, connections, and legitimacy of the global organizations would provide significant advantages to a G-20 based organization without necessarily including the overhead of an organization with more than 200 member states. Specific organizations to be considered include the International Telecommunications Union (ITU), Counter Terrorism Committee Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC), INTERPOL, the World Bank, and International Monetary Fund. These organizations have either experience in this specific sector as with the ITU, CTED, and UNODC or are key elements of the global financial system where the direct results of cybercrime are most visible. Several regional international organizations such as the Organization of America States and the Organization for Security and Cooperation in Europe have elements involved in supporting member state efforts in cybersecurity. The Internet Corporation for Assigned Names and Numbers (ICANN) must also be an active participant.

C. Recommended structure

The new body should have a structure similar to the current FATF. A small secretariat operating under an internationally appointed executive secretary would serve as the day to day entity of the organization. The secretariat would be charged with maintaining and publishing the official documents, coordinating meetings of the international group, and providing a stable point of contact for outside organizations and states. Basing the unit in one of the existing UN or OECD hubs would limit the need for additional complex logistical and administrative support structures.

The core of the organization would be the representatives of the member states. They would form the working groups and committees that develop the recommendations and determine their applicability. They would also be the nucleus of the mutual assessment teams key to validating member state compliance. These would be part time duties as required to support the working groups and assessments.

The committee of the whole, with voting rights vested in member delegation leadership appointed by the member organizations, would be the highest body of the structure. Leadership would be on a rotational basis among the full members for a set term. The group president would have the authority and stature to represent the group to the G-20 or other international organizations. This logically would require someone at the ministerial or vice-ministerial level. This person essentially provides the governmental legitimacy and accountability for the organization.

Of critical importance is the development of subordinate regional organizations similar to the FATF model FSRBs. The smaller regional based groups could be sponsored by existing regional forums or be independent. They would be designed similarly to the G-20 based body with a broader regional representation that includes key private and non-profit sector participants. Again there would be a requirement for small day to day secretariat and a decision making ministerial body. Technical assistance missions from donor states/organizations could be requested and coordinated via the regional bodies. Eventually these regional bodies would assume greater roles in providing assistance and mutual assessments as has occurred with the FATF organization. Participation as observer/supporters of regional bodies by members of the core group would be essential for success

D. *Required tools*

The internet security organization requires at bare minimum the tools necessary to establish a list of recommendations and the ability to enforce them. Integral to this capability is the generation of sufficient political will on the part of member states to implement the recommendations.

The recommendations should focus on disclosure requirement analogous to financial know your customer (KYC) requirements in the FATF recommendations. Verification of ownership of websites, ISP companies, servers, and similar items is essential for tracking down and holding violators accountable. Strong authentication and attribution is important. This arena is not without risk however. Much of the advantage of the freedom of communication and speech associated with the internet is based on its ability to maintain anonymity [15]. Current world events such as the revolutions in Egypt and Tunisia leveraged internet provided communications tools. Significant human rights violations are possible if identity information is abused by unscrupulous authorities. Any governance structure must provide for human rights protections.

A mutual evaluation regime must be part of the process in order to hold members to standards and to provide transparency to all concerned parties. If the group's seal of approval is not verifiable, it will not be worth as much to third parties and private sector investors.

Third, capacity building for lesser developed states is critical to success. In the internet borders do not readily exist. The weakest point of entry is most likely to be exploited and leveraged to allow access to others.

Fourth, and perhaps most importantly after building political will, there must be a mechanism to compel compliance. The FATF's name and shame policy directly enabled it effectiveness [9]. Isolating a poorly run ISP from the network or limiting traffic from nations not enforcing minimum security standards allows market pressures to be brought to bear to encourage providers and states to get involved in security. Legitimate business interests know the risks to their reputations and goodwill implied in dealing with illicit actors. International cooperation is necessary because no one country or company can secure the internet [15].

E. *Possible alternatives*

There are few viable alternatives on the international horizon. Within the United Nations process, the ITU has taken the lead in cybersecurity. The World Summit on the Information Society (WSIS) Tunis Conference charged the ITU with responsibility for coordination of the action items on building trust and confidence in ICT systems [17]. While the ITU Secretary General Hamadoun Touré made cybersecurity the ITU's top priority [17], little tangible progress has been made. The organization focused more on threat response and capacity building for lesser developed nations than on establishing international mechanisms to reduce threats.

The Internet Governance Forum (IGF), which developed from the WSIS process, may provide a forum but it lacks decision making authority [18]. While this process provides opportunity for discussion among all the stakeholders it lacks the power needed to effect changes.

The limitations of a cybersecurity treaty have already been discussed. While a robust treaty regime with an implementation and enforcement mechanism such as the Chemical Weapons Convention and its implementing arm, the Organization for Prohibition of Chemical Weapons, could be successful, the prospects of adopting such a regime appear very unlikely.

IV. CONCLUSIONS

Cybersecurity demands a global response. The internet is now a ubiquitous tool that has penetrated the everyday operations of government, business, and individuals around the world. Computers are no longer housed only in large buildings but carried in pockets. The ability to secure and safeguard the cyber domain has not developed as fast as the technology. Critical decisions about cyber practices and security technology need to be made, but the global organizations established thus far have not reached consensus or demonstrated the ability to take the necessary actions.

A new body, modeled on the successful Financial Action Task Force with a mandate to improve international cybersecurity, offers an alternative to the current chaos. The body should be chartered by the G-20 and include representation from the private sector and pertinent international bodies. The key to success will be the political will of the membership. A commitment to openness and willingness to implement best practices are requirements. Finally, the body must be able to recommend to its member states the corrective and punitive measures necessary to improve cyber domain security for all users.

ACKNOWLEDGMENT

I would like to thank the Director of the Center for Hemispheric Defense Studies, Dr. Richard Downie, and the center's faculty and staff for their support. Additionally, I would like to thank my family for allowing me the time to study and write.

REFERENCES

[1] M. Liebowitz," 5 cyber threats to watch for in 2011". Security News Daily. [Online] December 29, 2010. [Cited: April 10, 2011.] http://www.securitynewsdaily.com/2011-top-cyber-threats-to-watch-for-0378/.

[2] M. Schwartz, Matthew, Information Week. Information Week. [Online] April 7, 2011. [Cited: April 10, 2011.] http://www.informationweek.com/news/security/vulnerabilities/229401124.

[3] E. Mills, Study: cybercrime cost firms $1 trillion globally. CNET News. [Online] January 28, 2009. [Cited: April 10, 2011.] http://news.cnet.com/8301-1009_3-10152246-83.html.

[4] Council of Europe. Convention on Cybercrime. Council of Europe. [Online] [Cited: April 10, 2011.] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

[5] S. Schjolberg, "A cyberspace treaty: a United Nations convention or protocol on cybersecurity and cybercrime" Salvador, Brazil : United

Nations, 2010. Twelfth United Nations Congress on Crime Prevention and Justice, A/Conf.213/IE/7.

[6] G. Masters, “Global cybercrime treaty rejected at U.N.” SC Magazine. April 23, 2010.

[7] J. Zarate, "Harnessing the financial furies: smart financial power and national security, Washington : Washington Quarterly, 2009, Vol. 32, pp. 43-59. DOI:10.1080/01636600903235890.

[8] Financial Action Task Force. An introduction to the FATF and its work. Paris : FATF/OECD, 2010.

[9] Fighting terrorism the FATF way. Gardner, Kathryn. Denver : Academic Council on the United Nations System, 2007, Global Governance, Vol. 13, pp. 325-345.

[10] P. Vlaanderen, “Towards global coverage and compliance” [Speech]. Praia, Cape Verde : FATF, May 5, 2010.

[11] Financial Action Task Force. High risk and non-cooperative jurisdictions. FATF. [Online] 2011. [Cited: Apil 10, 2011.] www.fatf-gafi.org.

[12] J. Tull, "The Internet--testing the limits of global regulation" [Speech] Burgenstock, Swizerland : Commodity Futures Trading Commission, September 6, 1996.

[13] Internet World Stats. Internet usage statistics:the big picture. [Online] Miniwatts Marketing Group, April 5, 2011. [Cited: April 10, 2011.] http://www.internetworldstats.com/stats.htm.

[14] Royal Pingdom. Internet 2010 in mumbers. Royal Pingdom. [Online] January 12, 2011. [Cited: April 10, 2011.] http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

[15] C. Sund "Towards an international roadmap for cybersecurity" Emerald Group Publishing Limited, 2007, Online Information Review, Vol. 31, pp. 566-582. DOI 10.1108/1468420710832306.

[16] The Rendon Group. Conflicker Working Group Lessons Learned June 2010. Boston : The Rendon Group, 2011.

[17] International Telecomunications Union. ITU Global Cyber Security Agenda. ITU. [Online] October 27, 2010. [Cited: April 11, 2011.] http://www.itu.int/osg/csd/cybersecurity/gca/.

[18] A. Doria and W. Keinwachter, [ed.]. Internet Governance Forum (IGF):the first two years. 2009.