International Coordination for

Cyber Crime and Terrorism in the 21st Century

Introduction

The need for international technical coordination

Networked information systems are being rapidly adopted by governments and businesses worldwide to improve communications, operational control, and – ultimately – competitiveness. Reliance on these systems, especially where the Internet exists as the primary infrastructure, is likely to increase. It is a complex technical and political task for nations and their commercial enterprises to protect information assets and ensure that critical operations continue even if attacked. The growth of world markets and an increase in transnational mergers only serve to compound this complexity.

As it stands today, the Internet is vulnerable to attack. The attacks are hard to prevent and respond to, and the perpetrators often go unidentified. The Internet can be abused and misused, to the detriment of all legitimate users and only to the benefit of those with malicious intent. Without steps to make the Internet a safer and more reliable environment, the operation of our critical infrastructures will remain at risk. An international effort is required to improve the general state of information technology or *computer* security because with shared risks comes shared responsibility for protecting information and the technology for its storage and transmission.

Governments are recognizing the need to protect their information and critical infrastructures in response to these threats and are responding accordingly. Some governments recognize that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is significantly reduced. Besides the technological challenges this presents, the legal issues involved in pursuing and prosecuting intruders adds a layer of difficulty as they cross multiple geographical and legal boundaries. An effective solution can only come in the form of international collaboration.

In the United States, for example, Presidential Decision Directive 63 (a white paper on critical infrastructure protection) states, "Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.… The Federal Government shall encourage international cooperation to help manage this increasingly global problem."

In the area of law enforcement, the Internet constitutes a new patrol area in many respects. Unlike jurisdictions based on national and political borders, the digital information infrastructure does not have a central location in the physical world. So not only is responding to attacks difficult technically but also many of the accepted methods for practicing law enforcement are ineffective. Recent G8 (Group of Eight Advanced Industrial States) and OPEC (Organization of Petroleum Exporting Countries) activities are examples of increasing recognition of this international need. The problems that we must address to improve our critical information infrastructures require the involvement of diverse parties including governments, policy and lawmakers, law enforcement,

software vendors, the research community, and practitioners such as FIRST (Forum of Incident Response and Security Teams) members who have experience responding to computer security incidents. Attempting to address the problems in one group without input and feedback from the others is likely to result in flawed or incomplete solutions. Last year draft U.S. government legislation (the Digital Millenium Act) resulting from the World Intellectual Property Organization (WIPO) treaty resulted in a flurry of panic throughout the Internet security community. Practitioners, researchers, software vendors, and incident response teams realized that aspects of their work that address security flaws to reduce risk to our critical infrastructures might become illegal under the proposed legislation. This was clearly not the original intent of the treaty or the resulting legislation. This is just one example of the urgent need for ongoing communication among policymakers, technologists, and others to ensure that future policies and agreements on a national and international scale are practical and effective.

Information exchange and interaction among many parties is paramount to producing comprehensive and practical approaches and solutions to the complex problems faced. Simply bringing parties together is not enough. We need to consider the issues that must be addressed to support a global incident response effort and to reduce the likelihood, number, and extent of computer security incidents.

Current difficulties

Many network protocols that now form part of the information infrastructure were designed without computer security in mind. Without a secure infrastructure, it is difficult to avoid security problems and resolve computer security incidents. The combination of rapidly changing technology, rapidly expanding use, and new, often unimagined uses of the information infrastructure creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict.

It is inexpensive (the cost of a personal computer and Internet access), quick (less than a minute), and easy (using freely available intruder tools) for anyone to launch attacks against our critical information infrastructures. Conversely, it is expensive (international effort and funding), long-term (research, development, and deployment), and complex (technically and politically) to take the steps needed to *harden* the information infrastructure to make it less susceptible to attack, and to enable us to respond more effectively and efficiently when attacks do happen.

In general, incident response and computer security teams consist of practitioners and technologists who have a wealth of operational experience but lack authority to make policy and security decisions in their organizations. They also may have limited funding and lack professional recognition. This has negative consequences; a given team's organization may not allow enough staff to respond effectively to security incidents. Similarly, a team may not have sufficient authority to influence and ensure improved computer security and comprehensive response. Moreover, at this time, there is no infrastructure to support a coordinated global incident response effort, although there are a few components in place that can form the basis of this infrastructure.

A variety of issues must be addressed when considering how to promote an effective global incident response infrastructure. These include discussions about which organizations will coordinate and participate in the development effort, how current groups and forums can fit their mission and objectives into an agenda to create a global infrastructure, and what possible structures and mechanisms might be required and effective in the future.

The Melissa Virus attack underscores the lack of such a global response structure for incident response. Because individual teams focused on their individual or national response needs, there was no operational global response effort. Although the FIRST played an essential role in the early identification of the problem and was able to notify others (due to early reports shared among its member teams), it has no operational mission or funding and so was unable to facilitate further response.

A recommended approach

In recommending an approach to handling the problems of today, we propose a global role for the incident response and security teams. These teams should use the strength of their technical coordination today to link to the international organizations aimed at tracking trends and activity of cyber crime and terrorist groups. Possible ways of achieving this are outlined in this paper.

In the computer security incident response community, we have been successful at resolving international incidents where the following elements were in place:

- A common terminology between parties involved in the incident to include identification of the intruder's M.O., the technical attack details, and identification of the targets
- An understanding of the common and conflicting societal issues surrounding the incident
- Detailed knowledge of the relative technical skills of all parties involved in resolving the incident
- Up-front agreements on how incidents of a variety of types will be handled

For all of these recommendations contained in this report, use of a bottom-up approach will provide the best implementation in the short-term and allow additional experience in working cyber terrorism and cyber crime issues internationally. In addition, support from decision makers in the international community is required to support these activities.

It should be noted that this recommended approach is *not* necessarily dependent on international agreements or treaties between governments. While these agreements can assist in the formal identification and prosecution of parties perpetrating cyber crimes and terrorism, it is the technical cooperation that is necessary to make the identification possible. Today, that cooperation is not available at the cyber-technical level but only at the national intelligence level.

Current Practice for International Coordination

In this section, I will address the technical coordination of international computer security incidents and the basis for this coordination. The structure will address first reports of computer security incidents where the victim is well defined, then move into the sharing and analysis of indications and warnings. Other sections will discuss the emerging technical threats and how they are communicated, followed by one of the biggest technical challenges today – the tracking and tracing of cyber intruders.

Computer Security Incidents

Today, computer security incidents are reported to regional or national response teams. Frequently these reports are motivated by a desire to patch any vulnerabilities that were used to enable the attack and not by a desire to determine either the international scope or uncover the intruder. An exception is when the target is a government or other potentially sensitive site where the response depends on knowing the origin of the attack. In this case, the tracking of the

individual is frequently turned over to the foreign office or other international relations office for the coordination necessary to track the intruder.

Information communicated in computer security incidents is controlled by the direct participation of the regions involved in the incident. For example, if an American university is attacked and it is found that there are log files pointing to a system in Europe, the CERT/CC will contact the appropriate team in Europe and share information that will help it resolve the incident on its end. They will not in general share this information with the entire response community in order to maintain the confidentiality of the attacked site involved.

Similarly, if vulnerability information is discovered in the process of resolving an incident, this information is shared with the vendor responsible for fixing the problem, but the specific victim information is not shared unless the attacked site gives permission and wishes to be in direct contact with the vendor of the software containing the vulnerability.

Indications and Warnings

Frequently information is reported to incident response teams where there is not a specific victim or computer security incident but rather an indication that some activity may be ongoing in some other part of the community. There is currently no standard way of sharing that information, although sometimes this information is posted to a shared list of FIRST members. This is one of the main areas that needs drastic improvement in the future in order to effectively process cyber crime and terrorist indicators that may be detected within the incident response community.

Emerging Technical Threats

The sharing of emerging technical threats is one of the best achievements of late. Today, the FIRST organization sponsors technical forums on a periodic basis to discuss recent development in technical threats and vulnerabilities. While this is a valuable meeting for the incident response community, it is not open to other international experts to relate the technical trends to political or other international trends.

Track and Trace for Intruders

One significant problem with the tracking of malicious activity to its origin is that it requires the cooperation of many independent administrative domains operating internationally. This makes the creation of a universally acceptable technology solution unlikely (e.g., modification of the computer protocols and services to automatically identify the point of origin). Thus a reasonable approach to track and trace today is the combination of technically experienced personnel working with these administrative domains to gain their cooperation voluntarily to trace back malicious activity to the actual threat behind the activity.

With the volume of information gathered by the CERT/CC and other international response teams, it is likely that the network of these incident response teams will provide the best start to tracking the activity of intruders and other malicious cyber activity to determine the point of origin. While this can never be a guaranteed activity, putting together all of the international evidence related to a malicious activity will provide the best cyber evidence of this point of origin and perhaps help to distinguish between domestic and international threats.

In addition to the information gathered by incident response teams, the CERT/CC has a unique relationship with many of the Internet Service Providers (ISPs) and network operation centers that enable the CERT/CC to work with both victims and transport providers to track specific activity to its immediate point of origin. Then with its reputation of impartiality, the CERT/CC

can frequently work with the administrators of these sites to trace back the activity one step further to attempt to find the true place of origin.

Recommended Approach for International Coordination

Expanded FIRST role

There is an urgent and ongoing need to provide a global infrastructure to provide a fast, effective, and comprehensive response to computer security incidents on a local, national, and international scale. At this time, there is no infrastructure to support a coordinated global incident response effort.

The need for an international forum to respond to computer security incidents was recognized in the early 1990s and resulted in the formation of FIRST. Today, FIRST consists of more than 80 incident response and security teams from 19 countries and provides a closed forum for these teams to share experiences, exchange information related to incidents, and to promote preventive activities. Although other teams exist that are not yet FIRST members and new teams are continuously being established, for years to come there will not be enough teams to address the growing need for global incident response. Additionally, FIRST as it exists today is a voluntary organization with no operational element. As such, it provides an introduction service and meeting place for teams to establish trusted interactions, but it is not currently able to provide the necessary coordinated global effort or meet other needs, such as a more open flow of sensitive information and close collaboration to respond to widespread events.

Among the challenges to expanding the role of FIRST are lack of appropriate policies and procedures, lack of formal agreements, and the difficulty of gaining entry into the incident response community.

> **Establishing policies and procedures.** The pioneer computer security incident response teams, formed in the late 1980s, were faced with defining their own appropriate operational guidelines with little or no experience on which to draw from. It has taken years for these now-established teams to develop comprehensive policies and procedures for their internal operations. Today, newly forming teams are not much better off than the early pioneers were, as little documented guidance is available.
>
> Moreover, this same community as a whole is still sorely lacking in the area of policies and procedures to support operations among teams. The progress being made in this area is limited and slow. It is mostly limited to a few isolated groups of incident response teams who work together regularly and have a business need to reach agreement. Progress typically comes to a halt when teams become overwhelmed by the number of issues that need to be addressed before they can reach agreement–such as no common agreement on terminology, definitions, and priorities.
>
> **Forming cooperative relationships among teams.** Currently, many teams agree to cooperate based on trust alone; they have no supporting contractual agreements to provide the foundation for their interactions. In fact, it is even more complex than that, as in some cases trust has been developed between individuals from given teams. So when trusted individuals leave those teams, the trust relationship may go with them. This can potentially result in the isolation of teams that were once part of a cooperative incident response community. Additionally, the information communicated between two teams during an incident is not well defined. The extent of the information might depend on

who is involved, their experience with the other team involved, and the specific staff members who are interacting.

Gaining entry to the incident response community today can be a difficult and lengthy process. The community is ready to embrace new members, but it is wary of interacting with new teams unless an existing member of the trusted community can vouch for them. As a result, some new teams are in a "Catch-22" situation – wanting to contribute but needing to gain acceptance and mentoring from an existing member of the community before they can begin to gain broader acceptance. As most teams have no charter or funding to act as mentors to new members of the community, finding a mentor and introducer is not an easy task.

Moreover, because there is no formal mentoring process for new members of the community, the guidance given to new teams can vary widely depending on the experiences and time available from their mentoring team. As a result, the incident response community expands at a much slower rate than is needed, and the teams operate with a widely varying set of operations and standards. The community needs to ensure and adopt a sponsorship process that doesn't depend on the good will of individual teams and ensures that each team meets an agreed-upon minimum level of operational standards.

Today's approach is not reliable, does not scale, and it must be made more effective. It is critical to have a global response infrastructure to replace a less reliable system based on trust between individuals with a reliable and effective system based on global understanding/agreement.

Providing security information to constituents. Local response efforts dedicated to individual communities (based on geographical location, organizational entity, service provided, or other criteria) are imperative to ensure that we all have incident response services that are appropriate for our needs. Each community has its own specific needs to address including: technology base, language, time zone, and legal jurisdiction (organizational, local, national, and international). However, the need for local response efforts does not eliminate the need for communication on a broader scale. Intruders are international in their movements and activities and so we must pool our response activities to ensure that we can respond appropriately.

For example, only a small percentage of the current incident response community researches and generates original source material for security advisories and alerts that advise the community on preventing and recovering from ongoing intruder threats. Presently, the members of the incident response community as a whole are adept at tailoring this source material to best suit the needs of their constituents and redistributing the modified material through local distribution channels. The community is continuing to improve the quality of and the speed at which information in these alerts is provided. Communication channels must continue to broaden to reach additional stakeholders. A global incident response infrastructure would continue to provide support for and enhance these rapid alert mechanisms.

The limitations of FIRST were evident during the Melissa Virus. FIRST asked its membership about the impact of the virus on their constituency to produce a global view of the activity. Because of the voluntary nature of FIRST and FIRST's lack of funding, it took almost four days from the initial activity report to solicit and receive status reports and generate the global activity

summary. Even so, the resulting summary provided a global perspective of the geographical impact and spread of activity.

A global incident response infrastructure would be the most effective way to facilitate response and to ensure that information is exchanged securely. This approach helps to ensure that response is effective, reliable, and timely.

Information exchange and interaction among entities is paramount to producing comprehensive and practical approaches and solutions to the complex problems faced. Again, bringing parties together is not enough. We need to consider the issues that must be addressed to support a global incident response effort and to reduce the likelihood, number, and extent of computer security incidents.

Although FIRST has been effective at supporting incident response activities that cross organizational and national boundaries, it currently lacks the structure, formality, funding, and operational mission to support either a coordinated global effort or other needs such as a more open flow of sensitive information and close collaboration during widespread computer security events. The FIRST organization could potentially fulfill an expanded role. To improve and maintain information technology, network security, and ensure the survivability of the information infrastructure, it is essential that we strengthen its ability to do the following:

- Cooperate globally to monitor the state of computer security
- Identify trends in intruder activities and system and network vulnerabilities
- Provide information that enables the public and private sectors worldwide to gauge their computer security risks
- Help these sectors determine their priorities for addressing these risks

Below we outline three possible models for implementing a global infrastructure for incident response:

1. A Global Coordination Center
2. International Time Zone Coordination Centers
3. National Coordination Centers

A Global Coordination Center

A natural model to consider is the establishment of a single center to coordinate global response to computer security incidents. At least a two-level hierarchy would be established, with the global coordination center at the top level and the rest of the infrastructure at one or more lower levels.

While conceptually this sounds like a clean and simple approach, it is fraught with practical and political issues. We will only address here what we consider main "show-stopper" issues. Experience has shown that it is insufficient to designate a component of the incident response infrastructure and expect it to succeed. To be successful, a component must gain constituency, recognition, and trust. It is unlikely that any one organization (of any form) could be established that could gain the global recognition and trust of every nation in the world. As a result, a single organization providing a truly global coordination service is not a viable option.

International Time Zone Coordination Centers

Another frequently discussed model is the establishment of a number of international coordination centers located in different time zones around the world to coordinate response to computer security incidents around the globe. If these centers were run by a single organization, the result would be the same as the global coordination center described above. So this model needs to be viewed from a different perspective. The centers would act as peers and coordinate their efforts, but each would be separately operated and run. This also would result in at least a two-level hierarchy being established, with the international coordination centers at the top level and the rest of the infrastructure at one or more lower levels.

The community has some practical experience in establishing, funding, and operating such centers both in the USA (the CERT/CC coordination role) and in Europe (the EuroCERT coordination role). The discussion of the issues below are based on lessons learned from those experiences. The role is one of *coordination* in response to incidents and events and not one of operationally *handling* incident and events.

It is important to note that national teams have resisted the suggestion that a coordination team for a continent might take over the operational mission for a region. They believe that the operations should stay within the team, close to the constituency, where the funding is and where the language, culture, and laws are understood. However, in some instances national funding bodies have given funding to EuroCERT instead of to the national team, falsely believing the international coordination entity would be a substitute for any national incident handling effort.

The impetus for a European coordination center resulted from the recognition that limited coordination among European teams was taking place and also from a general feeling that a coordination center located in Europe (rather than the USA) was needed for practical reasons (such as time zone, culture, and knowledge of the operating environments of the European teams). After a number of meetings by teams in the region, a project was initiated to establish a European CERT Coordination Service.

Experience has shown that although it is possible to provide an operational incident response service on a national or international basis, provision of a multinational or global operational service has so far been unsuccessful. The reasons for this include the following:

- **Funding**. Nations fail to recognize the need to fund both a national service and an international one. The funding source of an incident response team has great influence on how that team will be perceived and trusted both nationally and internationally.

- **Authority and balance of power**. Nations want to be responsible for their own needs and do not necessarily want a coordination center for the continent becoming privy to their data. Additionally, hostility between nations in the same geographical region will inhibit or prohibit cooperation. The role of a continental coordination center brings responsibility, prestige, and recognition. As a result, many countries may want to take on the role, making it hard to reach agreement. As previously discussed, trust and respect must be earned; they cannot be designated or delegated. There must be consensus and buy-in on the location and host of the continental coordination center. It is not something that could be moved from country to country on a rotating basis.

  For the reasons described above, even if sufficient international coordination centers did exist to provide global coverage, they would not hand off responsibility for activities within their own constituency to another such coordination center. Effective collaborations between international coordination centers could not be enforced, and recommended guidelines could be set for inter-international coordination center collaboration. But as with any incident response team, if the centers themselves do not have mutual trust and respect, interactions will suffer.

- **Issues of scale** . Organizations have yet to address the practicalities of scale when trying to dig through a huge volume of data resulting from a global influx of information. When providing coverage for more than one country, cultural and language issues come into play (this can be an issue even within a single country). In the incident response field, it is vital to ensure that all parties involved understand what is being communicated. It is unreasonable to expect that each international coordination center would hand off coordination responsibility for activities relating to its constituency to another international coordination center. As a result, to be effective, each international coordination center would need to provide a basic level of services on a 24/7 basis. There are a number of practical issues that must be addressed when dealing with multiple time zones (such as shifts and coverage). It is hard to transition work from one time zone to another as the day passes around the world. Such transition will invariably result in loss of both continuity and productivity due to any "ramp-up" during the hand-off.

Although many coordination centers exist, truly multinational ones struggle to address the practical issues of providing operational service to a global community. We do not consider this to be a viable approach to address global incident response needs. However, if some nations can reach agreement and establish one or more international coordination centers, then these can participate as components in a global incident response infrastructure.

National Coordination Centers

The number of national teams is continuing to increase, and many other existing and newly forming teams have constituencies that fall within national boundaries. National boundaries provide a demarcation for policies, procedures, and jurisdiction for information exchange; thus, they provide an excellent opportunity for coordinating on a national level.

This approach is based on having every nation establish a national coordination center. This model is not as clean an approach as the first two and has its own limitations (described below), but it has more potential to achieve global coverage. Although these components need only provide a coordination effort, the centers might also undertake an operational incident-handling role, depending on the size of the nations involved.

One limitation of this approach is that there are teams (other than international coordination centers) that provide services to constituencies that cross national boundaries (incident response teams for multinational corporations). For this and other reasons, it makes sense to consider additional coordination boundaries to support such cases; coordinating centers might exist for teams with similar needs, such as those within the banking or telecomm communities. This would result in at least a three-level hierarchy. This hierarchy could be made flexible enough to enable teams, as appropriate, to be served directly by a coordination center without the need for national coordination. Issues to be addressed within this model include the following:

- **Funding sources**. Funding will come from different sources and will be dependent on the function provided by the team, the constituency served, and the team's position in the hierarchy. Participating teams will need to seek their own funding sources to support them as an infrastructure component.

  There is potential for funding from role two to provide support for infrastructure components to conduct sensitive/closed discussions. From an operational perspective, it would be possible to seek funding for groups of infrastructure components to collaborate and to provide funding for national/multinational organizations to develop tools and services to support the infrastructure (but not to run it).

- **Authority and balance of power**. Determining how to appropriately position a given team in the hierarchy can be addressed by a combination of approaches. In some cases, this will occur bottom-up because there will be components that do not wish to provide the funding to perform a coordination role. Some teams that gain the trust and respect of others may naturally find themselves being recognized in a coordination role. In other cases, the level in the hierarchy will result from existing organizational structures. However, recognition of national teams themselves will result not only from national designation, but also from international recognition. Until base standards are recognized in this area, the situation will remain complex and problematic. Many existing "national" teams are not truly national because their constituencies do not officially extend to a nation but, instead, to national academic and research networks.

  A neutral arbitration service will be necessary for the discussion and resolution of disputes between incident response teams at all levels. We suggest that this service be provided by the professional society component of role two.

- **Issues of scale** . For large-scale events that affect a significant number of sites across the world, this approach can become complex without a single team taking on the coordination effort for the event. Agreeing to allocate the coordination role "on the fly" would not be productive or efficient. It might be appropriate to identify and recognize a number of teams that are willing and able to take on such a role in advance.

- **Organizational requirements**. With such a large number of nations around the globe, a higher tier of coordinating teams will need to exist for this approach to work effectively. This

higher tier is likely to evolve from a limited number of international coordination centers becoming established for small groups of cooperating nations and other coordination centers representing specific interest groups and industries. In reality, we will have a web of incident response teams that have the flexibility of coordination on a number of levels.

Although this approach is not ideal, it may be the only possible approach that can be implemented on a global scale. There needs to be a way of reaching agreement on some of the issues described above before this could be implemented. A major hurdle that the infrastructure will need to overcome is the minimum level of standards that all participating can agree to from the outset.

Non-technical forum for discussion of societal trends and differences

Another important recommendation is to create non-technical forums for discussion of trends and intelligence information that is important to the incident response, cyber crime, and cyber-terrorism communities. This forum would be designed to link political and social trends to technical activity in order to obtain a global picture of cyber activity.

Conclusions

Our critical information infrastructures and the government and business operations that depend on them are at risk. We share the responsibility to improve Internet security and coordinate effective international global response to computer security incidents and events. To be successful, we must ensure participation and cooperation among governments, law enforcement, commercial organizations, the research community, and practitioners who have experience in responding to computer security incidents.