# PROTECTING USERS OF THE CYBER COMMONS

Stephen J. Lukasik
Center for International Strategy, Technology, and Policy
The Sam Nunn School of International Affairs
Georgia Institute of Technology, Atlanta, Georgia

## ABSTRACT

Progress in protecting users of the cyber commons, popularly called "cyberspace," has been slow since network services became a consumer offering in the 1990s. Protection of users from abusers and malicious actors is the result of several rate-dependent processes: technical innovation, market innovation, investments in protection services and products, imposition of government mandates, and achieving international agreements on technical standards and law enforcement cooperation. Rapid technical and market innovations have had the unfortunate result of creating vulnerabilities as they add functionality, while the investments and agreements that might deliver protection operate slowly. Vulnerabilities arise from unavoidable technical errors, from lack of knowledge or carelessness by users, by management failures to invest in protection in proportion to user needs or to operate facilities and services responsibly, as well as the development of a commercial malware industry. This paper points to top-down and bottom-up processes for protecting the commons. Those implemented to date have not worked sufficiently rapidly to prevent abuses from increasing. The paper proposes a new measure, based on the idea of social networks, to deliver protection more rapidly than those paced by the slow elements of the current protection process. It is a proposal to provide protection that is intended to "grow" using the same elements that grew the cyber commons: bottom-up user initiative within a framework of top-down decisions and mandates.

## INTRODUCTION

The issue of cyber protection has long been of concern: the Morris worm in 1988; widespread development of the commons through commercial email and web browsers in the early 1990s; and a U.S. Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996.[1] Google reports over 43 million articles dealing with computer and network security. This much attention leads one to wonder why problems persist. Are computer vulnerabilities growing faster than measures to reduce them? Perhaps the problem is not purely a technical matter of computers and software, but with their users. Carelessness in protecting oneself, tolerance of bug-filled software, vendors who sell inadequately tested products, and the unappreciated complexity of network connectivity lead to the current abuses of the commons.

The position taken here is that it is all the above. The causes and potential remedies are many. The current approach appears to go at them piecemeal, fixing the flaws that demand immediate attention. Since this is not keeping up, it may be useful to rethink the approach, to see if there are strategic directions that, if examined, might offer benefits.

Protecting users of the cyber commons, nationally or globally, has both top-down and bottom up aspects. Calls for government action to "protect cyberspace" relate to top-down processes that, while they identify drivers of policy, wash out lower-level detail. That is the way governments think and what people have come to expect of them. Protecting a national commons would appear to be little different from other aspects of national security, clearly a government responsibility. In the U.S., under the recently organized Defense Department Cyber Command, the National Security Agency has been designated as the U.S. cyber force.[3] This includes both the 24th "Air Force" and the 10th "Fleet," the quotes because these forces neither fly nor float. They consist of people at computers, the newest element of net-centric warfare.

Bottom-up processes are equally important. These are what "really happens," the way processes work. They are rich in detail but leave major drivers of events invisible. The difference between the two perspectives is the same as that between legislation and how the complex systems necessary for its implementation perform in practice. Complete descriptions of processes include elements of both.

This paper describes the contributions both aspects make to the goal of protecting users of the commons, large and small. Neither perspective by itself is enough. Effective protection requires both in combinations that depend on particular historical and cultural circumstances of jurisdictions.

## GOALS FOR CYBER THREAT REDUCTION INITIATIVES

W*hat* threats against *whom* should be reduced? Starting with *all users of the global cyber commons,* Figure 1 suggests some major classes of users who share common security concerns. Sovereign states have considerable jurisdictional extent and resources. Infrastructure operators and communication carriers can be a powerful group when they feel they have liability, responsibility, and authority. State, county, and local governments have responsibilities though they may not be not matched with adequate financial and human resources.

Private organizations that have operational features in common can provide market leverage as well. Examples such as educational institutions and health care organizations are linked by standards groups and industry associations. They can make investments in security through voluntary collective action such as best practices, analyses of security failures, and cooperative R&D.

These do little for the email, cell phones, text messages of individuals, or for game players, homes, small businesses, and special interest groups. Such users have neither the skills to protect themselves nor a deep awareness of security until they experience disaster. *Yet these users are the core of the cyber defense problem*. Their machines can be captured into botnets, to become remotely controlled attack machines capable of overwhelming defenses. While what each user has to lose individually from cyber attacks may be modest, collectively they

are the soft underbelly of the commons, a route to more globally significant targets. They are both victims and unwitting accomplices of attackers.

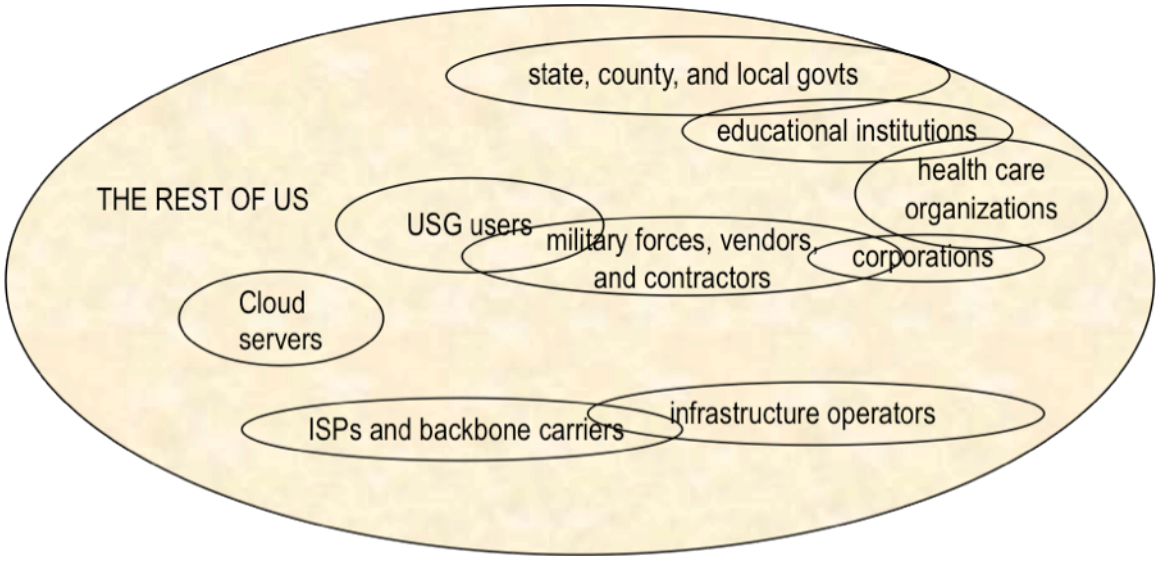


Figure 1
Typical Classes of Users of the Cyber Commons

While public and private programs can be justified when targeted to specific sets of users for particular purposes, they leave *the rest of us* to fend for ourselves.

A recent NRC study examined a number of research areas that relate to the above.[4] It offered a Cybersecurity "Bill of Rights" that define a set of user expectations:

> Availability of system and network resources to legitimate users;
>
> Easy and convenient recovery from successful attacks;
>
> Control over and knowledge of one's own computing environment;
>
> Confidentiality of stored information and information exchange;
>
> Authentication and provenance of information;
>
> Technological capability to exercise fine-grained control over the flow of information in and through systems;
>
> Security in using computing directly or indirectly in important applications, including financial, health care, and electronic transactions, and real-time remote control of devices that interact with physical processes;

Ability to access any source of information safely;

Awareness of what security is actually being delivered by a system or component;

Redress for security problems caused by another party.

Buried within the nouns and adjectives, e.g. legitimate, easy, convenient, confidentiality, authentication, fine-grained control, any, and redress, are knotty jurisdictional-dependent political issues. While we can complain that we are far from enjoying these "rights" in the cyber domain, how to achieve them in a global commons is by no means obvious. They are more like stars to navigate by rather than places one can expect to reach.

## A Top-Down Perspective on Protecting the Cyber Commons

The space of possible defensive actions has at least four dimensions: mandatory defense of cyber domains essential to the economic health and quality of life of people; national strategies, plans, and programs to coordinate defense of the commons; international legal regimes and supporting international structures to encourage and assist in defense of the commons; and technology to warn, prevent, and thwart misuse of the cyber commons.

There is no silver-bullet for the protection of the commons. The amount and type of protection of the commons will vary with the individual jurisdiction and over time as adversaries change, as technology changes, and as attackers refine their attacks and redefine their goals and targets.

o Mandated Protection of Essential Parts of the Commons Through Regulation

The regulation of private domestic activities is a function of states. Its intent is to enhance public safety, increase reliability, maintain law and order, and protect society from exploitation. Government-owned infrastructure should be subject to the same regulations, but the government regulates itself and thus has some flexibility compared to private operators. Those parts of infrastructure on which the public depends will require mandates through the agencies responsible for their oversight.

Regulation implies restrictions on the operation of markets and can foreclose potentially beneficial options. There is general recognition that infrastructure services merit some degree of regulation to protect against inequitable access to service and the abuse of what can be natural monopolies. Deciding what to protect defines what not to protect. By default, the latter are left to market forces to address. The decision should hinge on the allocation of resources to provide the greatest protection to the greatest number of people. This requires analyses of users, their relevance to national goals, and interdependencies among their needs. What we currently have is some mandated protection in some central infrastructures and national security assets, with the remainder dependent on market forces to strike the balance between security, cost, and convenience.

The PCCIP identified eight critical infrastructures. The U.K., in preparing for the year 2000 expected disruption of computers, identified eleven as central to the operation of society. The European Commission also identified eleven infrastructures. The infrastructures common to such lists, considering also their interdependencies, are telecommunications, electric power, and the transfer of funds.[7]

All infrastructures, as currently designed, depend on the reliable transmission of information for their minute-by-minute operation. If one is to protect any part of the cyber commons, protecting the command and control mechanisms of infrastructures is part of what should be done.

An illuminating example of the protection of a critical infrastructure is provided by the regulator of the U.S. electrical power system. The Federal Energy Regulatory Commission (FERC) has worked closely with industry groups such as the North American Electric Reliability Council (NERC.) A Final Rule, issued in 2008 provides a useful starting point.[2] While heretofore reliability has been treated as *desirable*, the *requirements* on the industry were flexible. The new regulation details actionable security processes for infrastructure protection that recognize both the realities of computer technology and the tendency of organizations to cut corners.

The FERC order is firm in blocking arguments that regulated entities can determine for themselves the level of risk they choose to accept, claims of the exercise of responsible business judgments, or challenges to the technical feasibility of regulations. With regard to the business judgment argument, the Report says The Commission noted in the Notice of Proposed Rule-making that *"cyber security standards are essential to protecting the Bulk-Power System against attacks by terrorists and others seeking to damage the grid. Because of the interconnected nature of the grid, an attack on one system can affect the entire grid. It is therefore unreasonable to allow each user, owner or operator to determine compliance with the CIP Reliability Standards based on its own "business interests." Business convenience cannot excuse compliance with mandatory Reliability Standards."*

Regarding the willingness of operators to accept risk, *"The Commission continues to view the term "acceptance of risk" as representing an uncontrolled exception from compliance that creates unnecessary uncertainty about the existence of potential vulnerabilities. Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards. The Commission, therefore, directs the ERO [Electric Reliability Organization] to remove acceptance of risk language from the CIP Reliability Standards."*

With regard to the technical feasibility, the Final Rule states *"The Commission adopts the CIP NOPR proposal and directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards …we note that the Commission did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment."*

The Congress attempted to extend this proceeding as far beyond the electric power system as possible, but the Commission drew the line at its defined authorities. *"The Commission is sensitive to the concerns raised by the Congressional Representatives regarding the severe impact that a cyber attack on assets not critical to the Bulk-Power System could still have on the public. The Commission, however, believes that its authority under section 215 of the FPA [Federal Power Act] does not extend to other infrastructure. Section 215 of the FPA authorizes the Commission to approve Reliability Standards that "provide for the reliable operation of the bulk-power system," which the statute defines as the facilities and control systems necessary for operation of an interconnected electric energy transmission network and the electric energy needed to maintain transmission system reliability. In addition, section 215(a)(1) specifically excludes from the definition of Bulk-Power System 'facilities used in the local distribution of electric energy.'"*

The most significant change in behavior being attempted by the FERC regards the matter of trust. *"The Commission proposed in the CIP NOPR to direct the ERO to modify Reliability Standard CIP-003-1 to provide direction on the issues and concerns that a mutual distrust posture must address to protect a control system from the "outside world."The Commission noted that interconnected control system networks are susceptible to infiltration by a cyber intruder and stated that responsible entities should protect themselves from whatever is outside their control systems … The Commission noted that a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates … Mutual distrust does not imply refusal to communicate; it means the exercise of appropriate skepticism when communicating. The Commission believes additional guidance on what this means specifically in current practice would help responsible entities to avoid these misunderstandings … The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."*

Such injunctions amount to saying, "From here on you must take cyber, threats to reliability, seriously and not ignore them when they are inconvenient." While it is still too soon to know how effective this new approach to infrastructure cyber security will be, one conclusion is that even in a minimum regulation environment, regulatory bodies have legal handles on cyber security in regulated entities that are otherwise lacking in most other parts of the cyber commons.

A recent study examined whether effective cyber defense can be provided by current methods of achieving cyber security or whether fundamentally different approaches must be explored.[10] It makes two proposals that have been avoided or rejected by most groups dealing with this problem: regulation and identity management. It notes, "We believe cyberspace can not be secured without regulation." Of its twenty-five recommendations, six relate to actions that should be required of infrastructures overseen by regulatory agencies, or the authentication practices required of critical infrastructures. These include allowing consumers to use government-issued identity credentials; requiring all businesses to adopt a

risk-based approach to credentialing; and to encourage risk-based processes over specific prescriptions.

The second proposal, to regulate digital identities, would eliminate anonymity from users in the interest of facilitating accountability for actions in the cyber commons. This would seem to be no different from identifying taxpayers and displaying license plates on vehicles. The downside could be to eliminate the use of the net for political protest, a socially important feature of the net. This could be addressed by allowing unlicensed users, not unlike unlicensed spectrum allocations, where it is understood no liability is incurred by such users and no accountability expected of them.

o National Strategies to Lead and Coordinate Protection of the Commons

Another necessary government component of the defense of the commons is a national leadership and coordinating role to enable private actions. It also has implementing roles in proposing legislation, enforcing its mandates, and as a defender of users of the commons too small or too weak to act effectively on their own behalf.[7]

While the U.S. government seeks to rely on public–private partnerships, the degree to which network abuse is increasing suggests additional mechanisms are needed. Since commercial organizations see computer security as costs and do not value the corresponding benefits, private efforts have to date been insufficient. Both sides of the partnership are failing to stem the abuse of the commons.[6]

Efforts by the Obama Administration suggest that this posture may be changing. In recent remarks Melissa Hathaway, representing the National Security and Homeland Security Councils, said, "The Federal government cannot entirely delegate or abrogate its role in securing the nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and *all levels of government have the responsibility to ensure the safety and well-being of citizens."* [emphasis added][5]

While government leadership is necessary for defending the nation from cyber abuse, it is indirect. There is a long distance between government strategy documents and effective protection of all users of the commons.

o International Mechanisms for Cooperative Defense of the Global Commons

Cyber abusers and their victims are widely separated. Actions against violators are helped by common standards of unacceptable behavior. Rationalizing laws globally makes sense but is time-consuming and eventually is limited by the speed with which each country adapts to new technical, economic, and political circumstances.

For effective international agreements it is necessary to have implementing mechanisms tp monitor compliance by the signatories to maintain a level of trust and confidence among them; enforce agreements should signatories depart from expected norms; resolve disputes among the signatories; address technical issues of definitions, standards, and forensic

collection as may arise; and render assistance to signatories to respond to technical challenges expeditiously. The process is slow as diverse signatories must be convinced of the need for proposed measures.

While many protective steps can be taken without formal agreements, if *global* changes in security are to be achieved, a larger international framework will be necessary for facilitating cooperation among signatories. Elements of such a framework for international cooperation, drawn from various international contexts and common to most international organizations are discussed elsewhere.[11]

As with the regulatory and government strategy dimensions of cyber security, international mechanisms have a role to play. Like them, they are not easily matched to the needs posed by a dynamic technology environment and aggressive and quick learners among those who would abuse the commons.

o Technology to Limit Abuse of the Commons

The view of many is that the current lack of security of the commons, and of the information contained within, is but a bump on the road of technical progress, one fixable by layering on more and better technology. Using technology to fix technology is questionable as a response to a problem whose roots lie deep in the ever-growing complexity of the entire network of technologies increasingly adopted by modern societies .

Were technology to change less rapidly, such an approach might have a chance of success. But problems arise when unexpected coupling between parts of large computer-based networks exhibit behaviors that, while following precisely from their programmed logic, cannot be completely anticipated. Large networked systems have so many internal states they can never be exhaustively tested, nor to date has proving their security been successful

Technology cuts both ways. It creates new power through enhanced performance in terms of size, speed, bandwidth, connectivity, and functionality. But as it "fixes" old problems and provides improved capabilities, it creates new problems, embedding them deeply within unverifiable systems. The matter is one of relative rates of change. If problems can be fixed faster than new problems are created, one can imagine achieving a satisfactory level of security. But when new technology introduces new problems faster than old ones can be fixed, the resulting divergent situation defies control.

When the cyber commons is threatened by malevolence, a new rate of change parameter is introduced. Attackers quickly reverse-engineer security alerts and patches to exploit the flaws before defenders can eliminate them. Thus the defender fix-and-install-rate must be faster than the attacker reverse-engineering-and-exploitation rate.

A current example of technological exuberance is "cloud computing." Users are encouraged to move their information and their applications from machines under their inspection and control, and which could conceivably become adequately secure, into a "cloud" of networked computers of unknown ownership, location, management, and security. Should users enquire

of the cloud's security gatekeepers about such matters, they are told "trust us." One can hardly refrain from asking, "Why?"

Technology is an enabler for regulation, national strategy, and international components of protection of the commons. Like them, it is necessary but not sufficient. It is part of the problem, part of the solution, and part of the landscape. Most importantly, behavioral changes by users will be needed to break this self-destructive technology cycle:

> Users should seriously revisit the premise that any two things are better connected than unconnected;
>
> Managers should recognize that entrusting the fixing of flaws to the people who created them has natural limits, and that perhaps the security problem is not a matter of minor execution errors but of major architectural errors;
>
> Decision-makers should recognize any computer can be penetrated, just as any building can be entered, and any object can be stolen;
>
> All would be well advised to replace trust with distrust as a default condition in all computer-mediated interactions.

These need not necessarily deter innovation, but they call for adjustments in the expectations for the technologies they enable.

## A Bottom-Up Perspective on Protecting the Cyber Commons

Voluntary legal self-defense efforts are also necessary, and these are inherently on a smaller scale than governmental approaches. They are most easily accomplished when organizations are large enough and smart enough to identify and implement cost-effective defenses. They serve to establish a market for protection technologies and the security professionals who understand options and risks, but often these remain classified or proprietary.

The question voluntary self-defense raises is *who* does the volunteering and defending? The answer depends on the technical knowledge available to users and the resources they can devote to something that is not their central focus.

Other voluntary user-oriented mechanisms, such as the Internet Engineering Task Force (IETF) have served the internet well, developing protocols to provide greater security, and fostering next-generation networks.[8] Computer emergency response teams (CERTs), industry information sharing and analysis centers (ISACs), informal regional system-administrator groups, software vendors, the Forum of Incident Response and Security teams (FIRST), etc. help, but it is difficult for them to stay ahead of attackers.

An element in voluntary defense is organizing "trust." The seeds of today's Internet security problems were planted when the ARPANET rapidly grew beyond its first small circle of

researchers.[11] Early generations of network users were homogeneous, cooperative, dedicated to developing networking technology and its applications, and had no reason to distrust or harm each other. With net growth have come larger numbers of users, users who have no knowledge of each other and who have divergent agendas. Distrust should replace trust, but the means of practicing distrust are poorly served by network technology created to support trusted users.

The *National Strategy to Secure Cyberspace* published in 2003 relied on the principles proposed by the PCCIP: voluntary actions, public-private partnerships, public awareness, international cooperation, and the central importance of critical infrastructure.[12] The Strategy saw cyber attacks as crimes for which, through due process, perpetrators would be identified and prosecuted. Vulnerabilities would be reduced through an unending search for flaws and their elimination by vendors, service companies, and computer owners and operators. It presumes that software flaws can be reduced, over time, to acceptable levels. The defensive concept was to distribute response capabilities to user organizations acting on their own behalf.

The security problems experienced today are significantly greater than was the case when the PCCIP issued its recommendations. Their proposals are not now sufficient. There is an over-reliance on government, and individual foot-dragging to establish the minimum organizations will be forced to do Another factor is the deep-seated view that security goals can not be achieved without federal R&D funding. While time has been devoted to negotiating treaties related to “cyber crime,” nations use the delay to strengthen cyber intelligence collection capabilities and to develop capabilities for offensive cyber conflict.

Nor does the law enforcement paradigm handle rapidly evolving threats and it fails under emergency circumstances. The prospect of zero-day attacks, such as are possible with viruses that rapidly evolve, as well as by an aggressive malware industry, are important. Changes in both the nature of zero-day threats, the uncountable vulnerabilities of systems, and the strong motivations of cyber attackers require warning systems to detect attacks with enough time to allow defensive responses. Defense must be managed in near-real time so that at least some attackers' goals can be thwarted.

A possible way of doing this exploits the nature of self-organizing social networks. It starts with the proposition that users have a role in leading efforts for their protection, not simply in accepting what others choose to do or not do in their behalf.

Social networks have two characteristics that mimic the development of early networks. They respond directly as participants receive value, and thus grow in directions and at rates determined by that value. And second, they have overhead costs that are met in various ways. Typically they ride on the internet, where users pay for their access and where participating web sites may be supported by advertising income. Some central management is needed to maintain the integrity of the social network. Facebook rules to protect privacy, open-source software, user-created wikis, and apps purchased from creators through commercial sites are illustrative of the informal, yet resilient, nature of such networks.

Proposed here is what might be called a *Commons Protection Union (CPU)*, a social network to recognize attacks in real-time and to provide information to users, or their service provider proxies, to enable them to disconnect from parts of the commons to contain a "disturbance" until it can be analyzed for its origin and characteristics and systems restored to full connectivity. Since the cyber security problem derives from connectivity, managing connectivity will be part of the solution.

The operation of such a function can be done much more responsively than is possible when responses to attacks are paced by the rate of intergovernmental agreements and the implementation speed of national response agencies. A voluntary and flexible approach is required, free of contested mandates. Being open and voluntary, governments could participate in increasing its effectiveness to whatever degree they choose. Real-time event information from users, private security companies who choose to participate, and such public information as governments choose to contribute, could enable the distributed examination of malware and attacks, and provide information to participants for rapid analyses.

The arrangement would make attack and on-going probe information available for the common good, the essence of a commons. On the basis of such real-time information, participating users could take such defensive actions as they choose. They could reduce load, route around congestion, disconnect from parts of the net, collect and preserve forensic information, and increase their hardness level, depending on their assessment of the real-time threat level and the criticality of their operations.

Carriers and internet service providers currently do some of this. The new elements are voluntary information sharing of global real-time data at the user level, provided by users or their proxies, and trusted third parties as consolidators. The high-level nature of traffic monitoring can be designed to yield statistical measures for automated diagnostics and decision-making while respecting the privacy constraints placed on the information by its contributors. Global traffic monitoring could include parameters to assess flow pathologies and detect anomalous patterns. The proposal is not unlike a missile launch detection and missile tracking system, but where the defensive components are distributed and user-controlled.

How might this be brought about? The same way many activities start on the Internet: someone starts and, if what they do is of value, the idea spreads. Such an approach can potentially spread at the internet speed of social network rather than government speed. The proposal is, schematically:

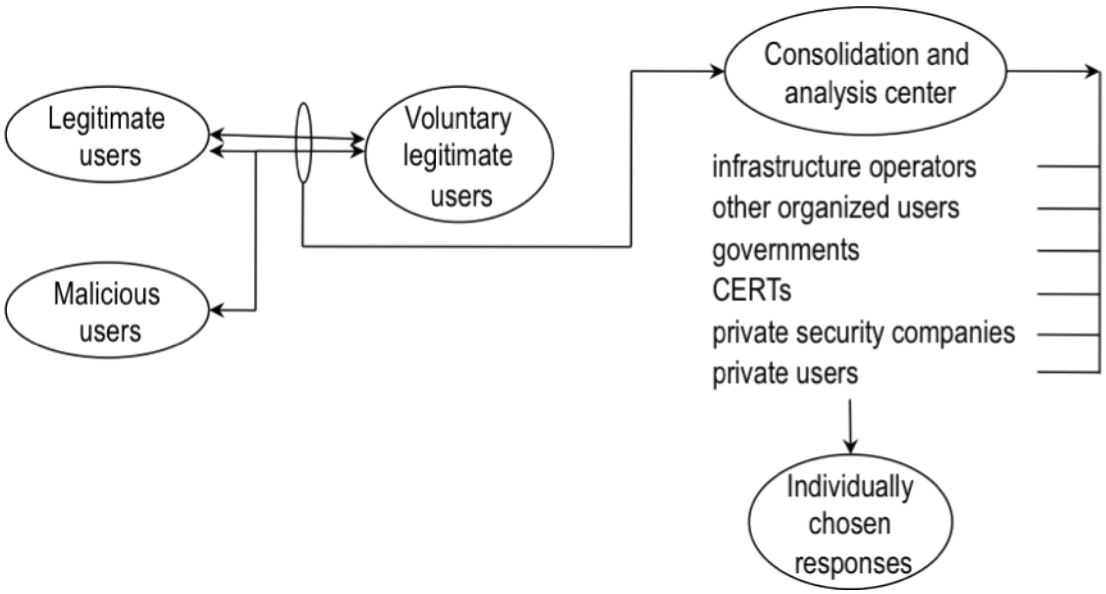


Figure 2
Schematic Concept of a Commons Protection Union

The upper-left shows the internet, with legitimate users dealing with other legitimate users. But now malicious users inject themselves into the internet masquerading as legitimate entities. Where the social network enters is that some internet users allow some or all of their traffic (externals or internals depending on choice) to be examined by independent agents (represented by a single Consolidation and Analysis Center in Figure 2.) Since participation is voluntary, and the data provided by users can be defined by them, privacy should not be an issue. Different participants and traffic from different domains can be treated separately. What will be important is who owns the contributed data, how securely it is stored, and its subsequent distribution, will have to be spelled out These data are analyzed for anomalies that can indicate the operation of a cyber attack or preparations for an attack. and the Center sends statistical information, or alerts of varying degrees of urgency to it subscribers who are able to respond in near real-time as they choose depending on the nature of the information and the nature of their operations.

There are various operational and business models for the process, several of which can be supported by different distributed agents. The CAC(s) would receive traffic externals from a number of user sources, of various types and locations globally. These would include such representative users as shown above: infrastructure operators, other organized entities, etc. So could be hierarchically processed flows such as ERO's might do for parts of the power infrastructure, nodes in upper levels of communication systems, feeds from CERTs, network security companies, and, most importantly, a representative set of private or small business users. Governments are likely to have their own systems for their needs but could participate with filtered flows should the choose to. The CAC could provide near-real time alerts and network status reports to users, with lengthier analyses following as more data are analyzed.

A CAC might be organized as a not-for-profit, supported by user consortia consisting of network affinity groups. It could function as a subscription service, with various levels of timeliness and depth of analysis. Amateurs perform similar services: ham radio operators in emergencies, astronomers searching for asteroids, or gamers finding approaches to protein folding. It could be a research operation studying network dynamics but also providing a real-time product, an objective that would also provide useful guidance for research. The output data could be used as a basis for further competitive for-profit value-added services. There is even a civil defense aspect that governments might support.

User volunteers would be responsible for delivering their selected signals to linked consolidation agents. Several CACs are possible having different governance structures. The basic governance principle, like the IETF, would be openness, rough consensus, and running code.

Attempting to analyze such a social network-based concept ignores its essential nature. Once started, through any of the several paths suggested, it will develop based on the degree to which it provides value to its participants. Existing social networks such as Facebook, Twitter, blogs, and wikis provide what in business would be called marketing and distribution.

There will be issues that will have to be addressed as a user-controlled network evolve. Participants will have to make their individual choice between privacy and the degree to which the social net demonstrably improves their protection. Its own defense will be necessary to avoid it being manipulated by the abusers whose activities it seeks to mitigate. Voluntary technical contributions needed for its operation will have to be forthcoming from the user community. The degree to which it works against the security products of its possible commercial participants will have to be balanced. It could give network abusers feedback on their effectiveness. It may be that the best capable and dedicated environment will be found in the same research community that formed the basis for the ARPANET. Such an experiment would be worth a try.

## ACKNOWLEDGMENTS

The author has benefitted from numerous discussions relating to improving cyber security with Seymour E. Goodman and Anthony M. Rutkowski. This study is based in part on a grant from Science Applications International Corporation to The Center for International Security, Technology, and Policy at the Georgia Institute of Technology.

## REFERENCES

[1] *Critical Foundations: Protecting America's Infrastructures,* Report of the President's Commission on Critical Infrastructure Protection, The White House, October 1997.

[2] FERC Order N. 705, "Mandatory Reliability Standards for Critical Infrastructure Protection," Docket No. RM06-22-000, January 18, 2008. The full document is at <www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf>. Individual security standards referred to are at www.ferc.gov/industries/electric/indus-act/reliability/cip.asp#skipnavsub.

[3] Gates, Robert M., Secretary of Defense memorandum, "Establishment of a Subordinate Unified U.S. Cyber Command under Strategic Command for Military Cyberspace Operations," June 23, 2009.

[4] Goodman, Seymour E., and Herbert S. Lin (eds.), T*oward a Safer and More Secure Cyberspace*, National Academies Press, Washington, D.C. 2007.

[5] Hathaway, Melissa, Keynote address delivered at the RSA Conference 2009, San Francisco, California, *The Obama Administration's Cyberspace Policy Review,* April 22, 2009.

[6] Internet Crime Complaint Center, Federal Bureau of Investigation and the National White Collar Crime Center, Bureau of Justice, Department of Justice. "2007 Internet Crime Report," See www.ic3.gov/media/annualreport/2007_ic3report.pdf.

[7] Lukasik, Stephen J., Seymour Goodman, and David Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack*, Adelphi Paper 359, International Institute for Strategic Studies, London (2003).

[8] Lukasik, Stephen J., "Protecting the Global Information Commons," *Telecommunications Policy*, Delft, Netherlands, 24, 519–531 (2000); this is a published version of "Next Generation Information Infrastructures," presented at the Next Generation Internet Conference, London, 21–23 Feb, 2000, London.

[9] Lukasik, Stephen J., "Why the ARPANET Was Built," to be published in the IEEE Annals of the History of Computing.

[10] "Securing Cyberspace for the 44th Presidency," Dec 2008. See <www.csis.org/tech/>.

[11] Sofaer, Abraham D., and Seymour E. Goodman (eds.), *The Transnational Dimension of Cyber Crime and Terrorism,*" Hoover Institution Press, Stanford University (2001). Chap. 4, Stephen J. Lukasik, "Current and Future Technical Capabilities."

[12] <www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.>