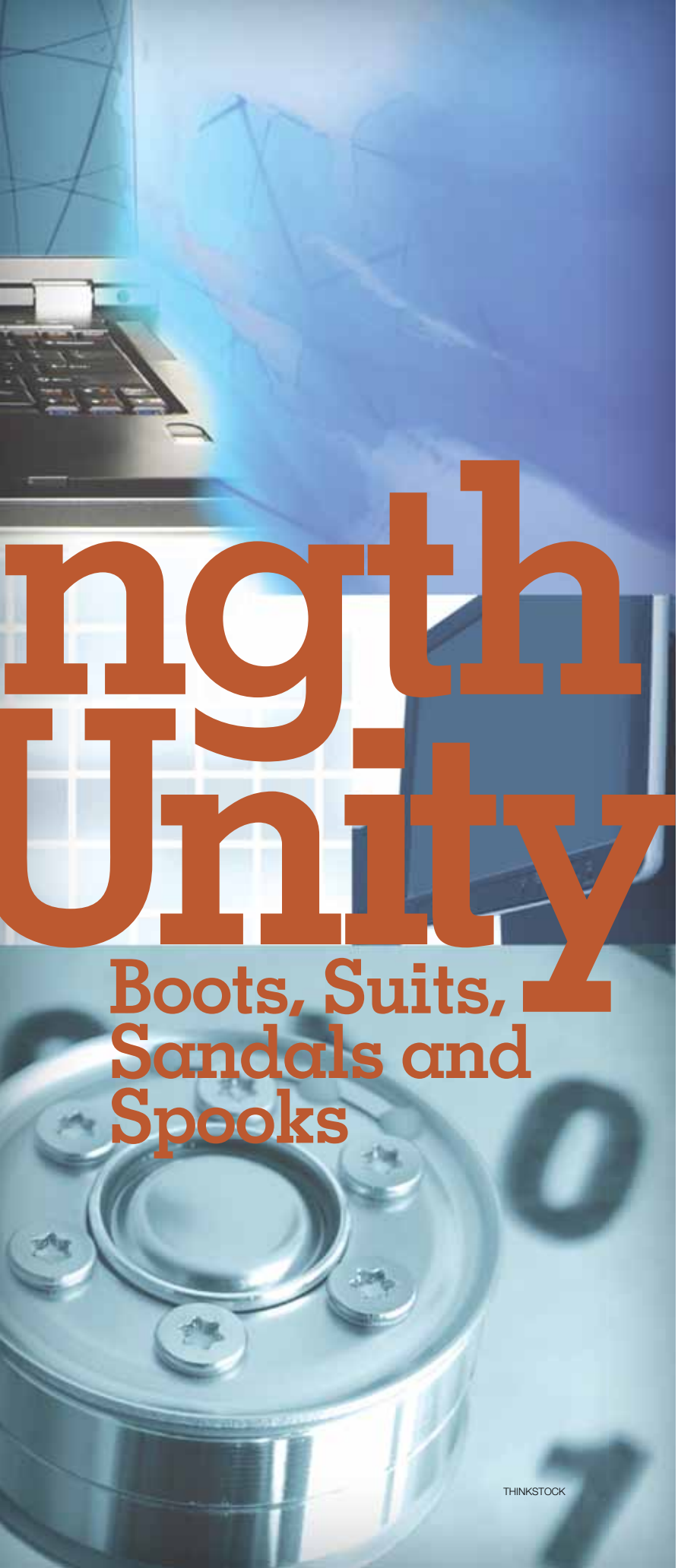

Stre
Through



ngth Unity

Boots, Suits, Sandals and Spooks

THINKSTOCK

Lessons from the Comprehensive Approach for Whole of Nation Cybersecurity

Alexander Klimburg,
Austrian Institute for International Affairs

A defining element of national cyber security is the importance of nongovernmental actors. For more than a decade, many governments have maintained Critical Infrastructure Protection, or CIP programs to encourage cooperation between government and certain key private sector companies, especially on cybersecurity. Results have been mixed, and there is a growing understanding that the wide-ranging involvement of nongovernmental actors is only possible within a "Whole of Nation," or WoN approach — a method of cross-organizational collaboration.

Within national cybersecurity, the importance of the private sector and civil society is obvious. The private sector is responsible for virtually all of the software and hardware that is exploited for cyber attacks, maintains most of the network infrastructure over which these attacks are conducted, and often owns the critical infrastructure against which these attacks are directed. Further, civil society actors — as distinct from the private sector — dominate cyberspace, defining the programmed parameters (i.e. the software protocols) of the cyber domain, as well as executing, researching and ultimately publicly speculating on cyber attacks. Together, these nongovernment actors account for the bulk of what is termed "national" cybersecurity. They are only partially accounted for in most national CIP programs.

Some critics, especially in the United States, may worry that the WoN approach allows the military a greater role in CIP efforts, as recently witnessed with the public activity of the new U.S. Cyber Command. There is some truth to this, but the criticism threatens to obfuscate a more important issue than the entry of the military into a mostly civilian domain. All relevant actors, in and outside government, need to be more involved in cybersecurity.

The difference between CIP and WoN is primarily related to scope. While CIP (when applied to cybersecurity) is concerned with defeating individual attacks, WoN cybersecurity is more concerned with addressing entire attack methods — for example, improving the quality of software to prevent errors in it from being exploited, or addressing issues of data retention and data sharing. Also, WoN cybersecurity has to address possible "catastrophic" cyber attacks on

national infrastructure, attacks that are likely to be waged within the context of cyber warfare. A reality of hostile acts in cyberspace is that some may well be state-sponsored, or even a first step toward cyber warfare. To be able to prepare for cyber warfare, it is therefore necessary to closely monitor purported cybercrime and cyberterrorist behavior.

While the WoN approach remains poorly defined within cybersecurity, similar approaches have successfully been implemented by a number of countries. Within the context of so-called Conflict Prevention or Fragile States strategies — which within the military includes stabilization operations such as in Afghanistan and Iraq —WoN has been employed for a number of years, even if not always under that specific name.

The NATO Comprehensive Approach is one such example of this approach in operation. There are many national doctrines as well, most notably in the United Kingdom, the Netherlands, Canada, Denmark and Finland, to name a few. The collaboration of defense, diplomacy and development actors is always paramount within these doctrines. This requires the joint cooperation of the military, political experts, civil society and intelligence communities — or "boots, suits, sandals and spooks" — to find common solutions not only at the operational level within the respective area of operations, but also at the political level within respective national capitals.

WoN refers to the joint integrated application of state (whole of government) and nonstate (business, civil society) efforts to attain a common objective. In Fragile States policies, this objective usually is the stabilization of a country or region. In cybersecurity, the objective is usually to decrease the vulnerability of a nation's networks

REUTERS

At the U.K. Government Communications Headquarters in Cheltenham, terrorism and cybersecurity take center stage in the country's national security strategy.

and critical infrastructure. In the next three to five years, a wide array of issues will need to be tackled in cybersecurity. A short list of hot topics would include data retention versus privacy, the liability of software companies, encouraging a nation's citizens to implement basic cybersecurity, the cooperation of critical network infrastructure owners, and, above all, information sharing within and between government and nongovernment.

To avoid reinventing the wheel in cybersecurity, it is advisable to learn from past experiences with whole of nation approaches. In essence, WoN is about process, and, like all processes, should be largely reproducible. Despite the seeming lack of communality between stability operations and cybersecurity, the two, after all, share one major common factor: the importance of working with nongovernmental actors.

REUTERS

A network defense specialist works at the U.S. Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado. National security planners propose that critical infrastructure such as power grids, communications and financial networks be similarly shielded from cyber marauders.

The Austrian Institute of International Affairs has researched different national WoN approaches on behalf of Austrian government clients over the past several years. Based in part on this research, a new Comprehensive Approach for International Operations (known as AEK: Auslandseinsatzkonzept) as well as the Austrian Program for Critical Infrastructure Protection, or APCIP are currently being formulated. Although an exhaustive "lessons learned" list would fill many pages, some common conclusions regarding the WoN process, especially related to CIP, can be made.

Top-down or bottom-up?

The need for top-level leadership to initiate the process, within the domains of both conflict prevention and cybersecurity, is a priority. While this may seem obvious, the considerable cultural barriers often encountered in WoN mean that top-level ownership is paramount. Different organizations can have entrenched interests that, at first glance, appear insurmountable. Only a top-down approach can have any hope in overcoming these obstacles, although building on the experiences of the operational base can prove useful. Indeed, sometimes the best approach involves "bottoming up" ("grass-roots approach") on the pre-existing working group-level networks.

This is particularly important when the goal is information sharing. Perhaps the most important tool in cybersecurity, information sharing involves the exchange of highly sensitive data, mostly on cyber attacks suffered and their consequences. In most of Europe, these exchanges are often referred to in general as Public-Private Partnerships, or PPPs, although such exchanges can also occur between government organizations and indeed between private businesses directly. In the U.S., the most prevalent form of cyber PPPs are known as ISACs, Information Sharing and Analysis Centers, which are maintained within specific industrial verticals, such as in power, water, finance and others. Although ISACs make a valuable contribution to U.S. cybersecurity, their initial years were problematic, in part because there was little senior-level buy-in from industry and virtually no attempt to connect with pre-existing initiatives. A similar model in the U.K., called WARPs, had more success because of support from business and government.

It is important to note that for military cyber warriors, some of the most important intelligence is generated in these groups. To get access to this information, it is necessary to participate in the exchange process. In other words, intelligence has to be shared with these nongovernment actors as well. One tested tool in this information exchange is known as the "Traffic-Light Protocol," although for some government actors this often requires legal changes in the way confidential material is handled.

Patiently building trust

In cases in which actors are unfamiliar with one another and start with considerable preconceptions, getting to know each other is important. This applies especially to the "boots versus sandals" group, development actors and the military, and data protection advocates and national security officials.

In the experience of this author, initial meetings can appear to go badly, but both sides nearly always agree to continue the dialogue. Subsequent meetings greatly contribute to mutual cultural understanding. This is a key requisite for any trust-building exercise and requires patience. Experience also shows that it is highly advisable to insist on group stability, meaning that the same individuals are present at each meeting.

It is important also to appreciate that "changing core ideologies" cannot be a deliverable of a WoN approach. Certain notions important to business and civil society actors, such as protecting intellectual property or preserving "humanitarian space," might seem to be at odds with the requirements of government actors. However, personal misconceptions can be changed, and often need to, if government and nongovernment are to work together.

In Switzerland, the highly successful cybersecurity organization MELANI (a government cybersecurity center that supports critical infrastructure protection efforts) had only a dozen private sector clients when it first went online. The private sector expressed concerns that seemed insurmountable. These concerns included data protection and private-sector doubts as to the overall competence of the public sector. Four years later, MELANI has several hundred clients — including most of the world's leading banks — and is highly regarded both at home and abroad. This trust was earned over a number of years. The benefits did not only apply to the private sector. As a result of this wide trust network, Swiss civilian and military cybersecurity operators possess some of the best cyber intelligence.

THINKSTOCK

Honest brokering

WoN efforts do not operate in a political-social vacuum, and will reflect common perceptions of the relative political power of the actors. Often, if not always, the state or public-sector will be perceived as the strongest political actor at the table. Usually it's the state that also will initiate the WoN process. Some of the other actors will initially be less convinced of the relevance of the process itself, and will treat most aspects of the process (including participation) as being contingent on negotiations in other fields as well.

As the initiating actor, the state has two choices on how to approach this delicate matter. It could behave as a *primus-inter-pares* (first-among-equals) actor. Here, the state directly seeks to represent its interest at the table as well as moderating the process. The advantage is that the state is directly able to engage with the other actors, and also places the outcome before the process. The disadvantage is that the state must be able to present a completely united front (i.e., if more than one governmental actor is represented, the respective hierarchy between them must be clear to all participants).

Also, the process might degenerate into "horse-trading" of the state with individual nonstate actors, failing to create any institutional buy-in on the part of these actors. Countries that have engaged in the *primus-inter-pares* role include, in particular, the U.S., U.K., and Australia. In each case, a single government agency or department was empowered to lead these discussions. In the U.K., for example, this falls within the responsibilities of the Centre for the Protection of National Infrastructure, or CPNI.

A second approach is to utilize an "honest broker" intermediary. This actor does not have a direct stake in the outcome and is therefore only concerned with the process. Often a nonstate actor, such as a think tank, is entrusted with the task through the state and occupies a hybrid role within the process.

An advantage of this approach is that by separating process and outcome, the process is endowed with a more impartial nature, arguably more conducive to creating a whole of nation mindset among the actors. Also, it is particularly useful when a number of government actors are at the table, and no one particular actor is able or willing to represent the state. The drawback of this approach is that the intermediary can overstate the importance of process over outcome, thus curtailing possible positive externalities, such as new initiatives. Also, the scope of individual negotiations is reduced, as the process is endowed with a more collective nature. An example of this approach is the National Institute to Combat Cybercrime or NICC, in the Netherlands.

Does a "big tent" approach work?

Transparency and inclusiveness have benefits, but also pitfalls. In case studies, there were striking differences between the small, select and confidential approach versus the "big tent" approach. Evidence suggests it is better to start small and later go big.

In cybersecurity, there have been clear indications that the small-group approach is more likely to pay dividends. For example, as the U.S. Deputy Secretary of Defense William Lynn recently discussed, U.S. Cyber Command has pioneered a number of new security measures, such as the introduction of automated active defenses against cyber attacks to protect the defense industrial base. These results were mostly possible due to close collaboration between the command and a few defense contractors.

On a smaller, tactical level there is often common understanding that smaller groups are much better at information sharing than larger groups. Both the CPNI and the NICC, for instance, cap membership of a particular group at no more than a couple dozen participants.

However, WoN seems to imply the need for much wider participation than is currently covered in conventional CIP programs. Unlike CIP programs, WoN is supposed to deliver much wider changes in policy than the "operational measures" described above. For example, how would government motivate software companies to take more responsibility for the integrity of their products, given that the majority of cyber attacks are delivered through errors in their programs? How would it persuade more private businesses to contribute to national cybersecurity by sharing data? These issues cannot be tackled in small, secret working groups, but require widespread consultation and political support, even if it can be helpful to consult earlier with a select group.

In conflict prevention, this approach has already paid dividends. In one country examined, civilians and government initiated a confidential consultation process named after a local beachside hotel. One outcome was the civilians' tacit support for military engagement in Afghanistan. Another outcome was a wide-ranging public discussion on development and development aid, and how it should be best employed. A result of this public discussion was that even during the upheaval of the recent financial crisis, the humanitarian and development aid budget remain untouched. Clearly, the public discussion, which proved beneficial to the community as a whole, was only possible with the small-group trust-building and experience-sharing that preceded it.

While there are additional lessons learned than those described above (and include multiple caveats), these illustrate that the WoN approach is indeed a process, and like all processes should be replicable in different circumstances. The "boots, suits, sandals and spooks" do not always represent exactly the same actors. For example, the "sandals" can refer to development workers as well as bloggers. Also, the private sector is decisive within CIP, while in conflict prevention nongovernmental organizations are the main nonstate group. However, in both cases the principal issue is the broad cooperation of traditionally antagonistic actor groups.

Overall, the WoN process represents a paradigm shift in how security policy can be conducted in liberal democracies, a paradigm based on trust, common interest and the increasing reality of distributed power. □