Why the cyber-revolution still lacks a global rulebook

Cyber-space resounds to a cacophony of voices. More and more people are thinking about cyber-security, but many admit to being flummoxed by the complexity and fast-changing nature of the issues.

Among the radical changes on the cyber horizon are shifting demographics. The U.S. at present represents 19% of the global internet, but this is shrinking fast as connectedness increases worldwide and the centre of gravity moves south and east. As Canadian cyber-specialist Rafal Rohozinski puts it, "the poor developing countries are changing the culture of cyber-space." In Kenya, for instance, 99% of new internet connections are by young people using mobile phones.

So what needs to be done, and by whom? What rules and norms are being advocated by different countries, corporations and international agencies? On behalf of the Brussels-based think tank SDA – the Security & Defence Agenda – I set out to interview some 80 cyber-security experts worldwide in government, companies, international organisations and academia.

The SDA report *Cyber-Security: The vexed question of global rules* (www.securitydefenceagenda.org) has just been published, and offers a global snapshot of current thinking about the cyber-threat and the measures that should be taken to defend against it. For the moment, the "bad guys" have the upper hand – whether they are attacking systems for industrial or political espionage, or simply to steal money – because the lack of international agreements allows them to operate swiftly and mostly with impunity. Protecting data and systems against cyber-attack has so far mostly been about dousing the flames, but not fire-proofing the systems.

Brigid Grauman is the author of *Cyber-Security: The Vexed Question of Global Rules*, the in-depth report released in February by the Brussels-based think tank the Security & Defence Agenda (SDA)

Even if everyone accepts the need for standards, rules, laws and possibly a global treaty to protect cyber-space against cyber-crime, not everyone agrees on how to get there. The debate is also about who should make the rules, and to what extent dominance by the military is a good or a bad thing. The fact that cyber-space knows no borders implies that security is only as good as its weakest link, and that something must be done about unregulated countries that offer a haven to cyber-criminals.

My SDA report reflects sharp divisions over the rights of individuals and states in cyber-space. Most Western countries believe that

freedom of access to the internet is a basic human right, and that people also has a right to privacy and security that should be protected by laws. Germany in particular believes in protecting personal data over the needs of intelligence. UNESCO argues that the right to assemble in cyber-space comes under Article 19 of the Declaration of Human Rights.

At the other end of the spectrum are those countries, like Russia and China, that favour a global treaty but nevertheless believe that access to the internet should be limited if it threatens regime stability, and that information can also be seen as a cyber-threat. "The Chinese talk about information-security, we talk about cyber-security," one leading expert said. For these countries, any state has the right to control content within its own sovereign internet space.

Linked to the rights and responsibilities of states is the thorny issue of attribution. There are those countries – the U.S. loudest among them – that say that identifying a specific attacker is virtually impossible, and that the focus has to be on defensive systems. Others argue that attribution requires international co-operation, the sharing of information and assistance from local authorities. Some countries believe that co-operation is a threat to their sovereignty; others say they can't be held responsible for the activities of individuals or private companies; and a number apparently fear openness because they don't want to see restrictions on their political or military objectives.

Some clear themes emerge from the report, and they are issues that need fairly urgent resolution. Among these is how and to what degree should a more proactive, some would say more bellicose, stance be developed both in the military and private sector arenas. They also include the need for much greater international co-operation; introducing a more solid security architecture to the internet; and establishing cyber confidence-building measures as an easier alternative to any global treaty, or at least as a stopgap measure.

Each country approaches cyber-security in its own way. Some, like the U.S., Australia, the Netherlands and the UK encourage much more open exchange with industry. The U.S. is increasingly looking at the cyber-threat as another form of warfare, and preparing to respond aggressively.

But before there can be fruitful and transparent discussion of global rules, a very elementary problem must first be resolved; it is exactly what we mean by terms like cyber-war and cyber-attack. When identifying a cyber-attacker is so tricky, and when it isn't clear whether an attack is for political espionage or money-making purposes, or both, the sooner there's a common understanding the better. ■

Cecilia Malmström
EU Commissioner for Home Affairs

"If we are to keep an open and secure internet we have to act now"

Vint Cerf, one of the internet's founders, recently made the very interesting remark that "when we built the framework for the web, we didn't think about security. We should have put stronger focus on issues like 'Where did that email come from?' and 'What device am I talking to?' My conclusion is therefore that we should start again with the internet."

Starting over with the internet is hardly feasible, but Cerf addresses an issue that many of us are now uncomfortably aware of: we haven't taken the internet's security aspect seriously enough.

Let's say, for example, that one registers a domain name or an IP (internet protocol) address as Mickey Mouse, Main Street, Disneyland. This light-hearted example quickly loses its frivolity when we discover that almost 50% of the applicant data for the top five generic domains – .com, .org, .net, .info and .biz – shows false or incomplete identity information. This makes it extremely difficult, if not impossible, for law enforcement authorities to trace abuse of internet resources.

Equally worrying is the fact that anyone can now purchase illegally obtained information like credit card details from websites for as little as one euro per card. As it becomes increasingly difficult for anyone to prevent sensitive or personal information from being stored on the internet, we are all becoming vulnerable to these attacks.

Yet there are some who still insist that threats from cyber-space are exaggerated, and that with faith in technological advances and a little patience our security concerns will fade. I disagree; this is a battle we may not win. If we are to keep an open and secure internet we have to act now.

The main bulk of responsibility for this lies with member states and with industry. But the European Commission also has a role to play, and it's one we take very seriously. Enhancing cyber-security and tackling cyber-crime has been one of our top priorities since February 2010, as has been highlighted in the Internal Security Strategy. And much has been done both through harmonising legislation and also through practical actions.

But instead of focusing on what's already been done, we need to look ahead to see what's still to do. First, and to my mind foremost, is making all necessary preparations for the establishment in early 2013 of a European Cyber-crime Centre as the focal point for Europe's fight against cyber-crime. We are currently working on a proposal that covers the key objectives and logistics for the centre, and once finished this will be discussed with member states and industry. But as the old saying goes: "you only get out what you put in", so the centre will only be able to fulfil its potential through effective information sharing with partners.

Also lined up for this year is an overarching EU cyber-space strategy, to be developed by me and my colleagues Neelie Kroes and Cathy Ashton. It will aim to increase the impact of our actions, and above all to co-ordinate our activities more effectively. Links should be created between the cyber-crime centre and member states' law enforcement authorities,

and between different computer emergency response teams (CERTs). Through this, we will also improve co-operation between our two key agencies, Europol and ENISA.

But even if we step up our efforts in Europe, this will not be enough in terms of the global scale of the problem. And this is where co-operation with our strategic partners is crucial. The EU-U.S. working group on cyber-security and cyber-crime, set up following the November 2010 summit, and re-mandated in the 2011 summit, is a prime example of the type of co-operation we need.

The working group can be proud of its successes to date. It has successfully delivered results in everything from combating child pornography – where we have identified new technical solutions – to the first-ever test of transatlantic responses to cyber-attacks, an exercise that was held at the end of last year.

It is clear that much has been done in this field. But more remains to be done, such as making it more difficult for "Donald Duck" to register a domain name and improving operational co-operation in the fight against cyber-crime. This year the Commission will be busy working on all the plans I've mentioned, but wider support will be needed to ensure that these come to fruition. That's why governments, organisations and industry need to put cyber-security and cyber-crime higher on their agendas. And let's agree on one thing: more action is needed on all fronts. ■

Lars Nicander
Director, Swedish National Defence College's Centre for Asymmetric Threat Studies

"Cyber-security is high on today's global policy agenda, but it is not new"

Today there are two parallel approaches to strengthening safety and security in cyber-space: one is top-down and the other bottom-up. The top-down version focuses on international law and security policy, and is primarily concerned with designing and implementing rules of engagement when tracing malicious cyber-attacks. The bottom-up strategy involves international exchanges of best practice for handling IT incidents, either through technical Computer Defence Exercises or by creating joint, cross-border education programmes within regional hubs. An example of the latter is the informal Nordic-Baltic Hub, created by the Swedish National Defence College and the NATO Cooperative Cyber Defence Centre of Excellence in Estonia.

Cyber-security is high on today's global policy agenda, but it is not new. In 2000, two U.S. professors, Abraham Sofaer and Seymour Goodman, proposed an international convention on cyber-crime and terrorism in a paper which drew comparisons with the legal framework and structures that effectively rid the world of civilian plane hijackings in the 1970s. Back then a relatively small body, the UN International Civil Aviation Organization, was created by a General Assembly mandate to establish security and safety regulations for all airports with international civil passenger traffic. If host countries failed to comply with the new rules, international carriers stopped landing at their airports. As a result, the problem was more or less resolved within 18 months.

The thrust of the case made by Sofaer and Goodman remains relevant today, especially as non-UN bodies such as the Council of Europe, the Organisation for Economic Cooperation and Development (OECD) and the G8 do not have the necessary reach to deny safe havens to the spectrum of actors with malicious intent in today's cyber-space. ■

Adam Rapacki
Former Under-Secretary of State, Polish Ministry of the Interior

"On current trends we can expect further growth in the use of advanced IT to commit crimes"

Despite the many benefits of the internet, cyber-space plays host to an ever increasing number of threats to state security and new types of electronic crime. More and more criminal groups are transferring their activities to the virtual world, which they see as a source of quick and relatively easy income.

On current trends we can expect further growth in the use of advanced IT to commit crimes, perhaps extending into new fields of social and economic life. The internet may be used for blackmail, for example, with criminals threatening to exploit security gaps in computer systems. The fraudulent use of stolen digital information is another "growth industry". Attention must also be paid to online distribution of content promoting terrorism, Nazism and xenophobia.

For the Polish state, the most important thing is the security of critical infrastructure, in particular IT infrastructure, which is now fundamental to the functioning of government. In Poland, the body in charge of this is the Internal Security Agency. For many Poles, however, the biggest problem is the growth of trade-related cyber-crime, which generates very high financial losses.

The most serious threat in this regard is the predicted increase in fraud on internet auction sites. The largest such portal in Poland has about 11.5m registered users, with an estimated 160m articles sold in 2010. With 16m Polish homes already online – another figure on the rise – researchers at marketing institutions forecast that e-auction transactions will replace many traditional forms of trade.

Our unlimited access to the vast global resources of the internet mean we must expect other types of cyber-crime to develop rapidly; various forms of fraud, phishing crimes – where classified online information such as passwords or credit card data is stolen – electronic spying, distribution of child pornography, human and narcotics trafficking, the sale of stolen goods, violation of intellectual property rights and crimes related to unauthorised access to digital information and identity theft.

To reduce these threats it will be necessary to provide law enforcement agencies with the resources to fight cyber-crime effectively, including appropriate co-financing to allow them access to the most modern technologies for prevention, detection and prosecutions. Equally important is a suitable legislative environment, one which keeps pace both with technological developments and new categories of internet crime.

Another key issue is international co-operation. The number of "real-time"

economic cyber-crimes is ballooning and this requires fast cross-border responses. In the first half of 2010, for instance, Polish law enforcers initiated 881 proceedings on economic cyber-crimes, a figure which jumped to 1,220 in the same period last year.

Effective law enforcement – whether dealing with cyber-threats to the state, commercial users or home computers – will also require public-private partnerships with telecommunications operators and companies providing electronic services, as well as researchers and scientists working in the advanced technology market. Without such partnerships, we will be unable to provide appropriate protection to state or self-governing institutions, the commercial sector or private citizens. ■

Stefano Trumpy

Digital 'Sherpa' for Italy to the 2011 summit of the G8

"The field of cyber-security is so vast and complex that it needs multiple, specialised agencies"

The field of cyber-security is so vast and complex that it needs multiple, specialised agencies to tackle different facets of the problem. Where criminals are using the internet to perpetrate crimes in the real world, national and international law enforcement agencies have to be involved in cyber-detection. But different skills are required to defeat "malware" attacks on cyber-infrastructure and critical resources connected to it. Hence, as the G8 declared last year, internet security "requires co-ordination between governments, regional and international organisations, the private sector and civil society."

This multi-stakeholder approach is essential to improve confidence among both network users and providers in the safety of digital services such as e-commerce and banking. For the private sector, this means investing in security, adopting technological aids and promoting awareness of security threats among users. For users, it means actively participating in awareness campaigns and being proactive in the face of potential threats. Governments, too, have a role to play in helping to develop norms of behaviour and common approaches in the use of cyber-space. To be effective, however, all stakeholders have to provide the appropriate follow-up in each of the relevant, specialised cyber-security forums. ■

Melissa E. Hathaway

Former acting senior director of cyber-space, U.S. National Security Council

"Internet Service Providers are the front line of cyber-defence"

Thieves, voyeurs, spies and other nations regularly invade the electronic borders which surround our homes, businesses and government institutions. But because the job of safeguarding these borders falls between the twin public duties of securing economic progress and protecting national security, governments around the world can't decide which ministry to put in charge

of internet security. What they ought to recognise, however, is that Internet Service Providers (ISPs) – and more broadly the whole communications sector – are the front line of cyber-defence, and should therefore shoulder more of the responsibility this entails.

Major telecommunications providers and ISPs have unparalleled visibility into global networks. This enables them to detect cyber-intrusions as they form and head towards their targets. ISPs already adhere to common protocols and enable seamless, global connectivity, and collaborate to ensure uninterrupted service. They also limit the amount of spam reaching customers' in-boxes, notify users of botnet infections and partner with law enforcement agencies to block child pornography.

Why, then, don't governments expect ISPs to reduce the proliferation of malware and help eradicate infections on critical infrastructures?

What is needed is a holistic approach by governments around the world, with policies, laws and regulatory frameworks that support the communications sector and ISPs as they provide security to ensure the internet remains a public good.

Agreed international codes of conduct could, for example, require ISPs to inform customers whenever their computers become infected, assist in the eradication of infections or identify perpetrators. ISPs could also be required to report statistics to governments, educate their customers about cyber-threats and warn them about risks to internet transactions. In short, a collective global agreement could help make sure ISPs provide a reliable conduit of service, through which transactions can be maintained with integrity, confidentiality and privacy.

In this, cyber-space is just like any other essential sector where government regulation helps to maintain safety standards. In the food and water industries, for example, government inspectors help businesses keep bacteria and toxins within acceptable limits. In transport, parcel delivery companies and airlines have to check the goods they handle to prevent the transit of hazardous materials. There are plenty of other examples where governments regulate for the benefit of society at large. Cyber-security is no different. ■

Jaan Priisalu
Director General, Estonian Information Systems Authority

"If we make data as transparent as possible, digital freedom will create more secure societies"

Cyber-security and digital freedom are often presented as mutually exclusive, with data either being "free" or "protected", so that the only way to guarantee one is to sacrifice the other. I believe this is wrong; technology amplifies the objectives of a society. In an open society, it can support the free exchange of information by governments, companies and people. In a closed society, it can make a bad situation worse.

Many people worry that digital technology will allow the state to become a nosy "Big Brother", and want all data to be classified to protect their privacy. In reality, the system works the other way round. Where digital freedom is limited, a few privileged people are able to access restricted data without fear of being caught. This makes IT networks less secure for the majority, not safer.

In Estonia, on the other hand, all public data are

exchanged through X-road, a secure information transportation layer capable of logging the metadata of each access request. This allows people to see who is looking at their data, and if they have any concerns they can ask the relevant organisation to investigate.

Encryption is another example of technology that reduces inequality in society. In years past, only a privileged few had access to encryption technology; today more and more people can share encrypted data, and that's good for spreading democracy.

Encryption is also a solution to the problem of balancing people's demands for both digital freedom and cyber-security. With ID-cards, files can be signed and encrypted so that they can only be opened by the correct recipient. This system is available to all ID-card owners and increases cyber-security as well as digital freedom. In short, technology can enhance both openness and cyber-security. If we make data as transparent as possible, digital freedom will create more secure societies. ■

Stefan Wallin
Finland's Defence Minister

"Finland aims to become a global forerunner in cyber-security by 2016"

Cyber-threats are without doubt a new security challenge. Like most countries, Finland is increasingly dependent on a secure and functioning cyber-space and therefore increasingly vulnerable to unexpected and rapidly-emerging cyber-attacks. That is why we aim to become a global forerunner in cyber-security by 2016.

To this end Finland is preparing a comprehensive national cyber-strategy to ensure that the state and private sectors can work together to keep vital services operating under any circumstance. While this will be the first such national strategy of its kind, the overall approach builds on decades of co-operation and co-ordination in crisis preparation and management.

The guidelines for the new cyber-strategy were laid down in 2010 in the government's broader Security Strategy for Society. Finland's public and private sectors have traditionally co-operated to prepare for exceptional circumstances and work together effectively during crises. Being a key element in Finland's national security, this is known as the comprehensive security approach.

At the moment, however, responsibility for cyber-security remains scattered between many different organisations and stakeholders, reflecting their specialist areas of expertise. This has slowed the creation of common objectives, with key decision-makers acting in relative isolation. Procedures and responsibilities during a nation-wide cyber-crisis have also yet to be defined with sufficient clarity. One of the main tasks of the current process, therefore, is to assess the need for a new authority to co-ordinate the strategy at a political level, as well as organising responsibilities at the operational level.

Many of the risks of cyber-attacks are shared between the government and the private sector. And since most of the critical infrastructure is owned by the private sector, the job of identifying and managing cyber-risks must be done in partnership. The forthcoming strategy will respond to all of these challenges by comprehensively analysing cyber-threats and deciding on the best way forward. ■

Vytautas Butrimas
Chief Advisor for cyber-security, Ministry of Defence, Republic of Lithuania

"It is time governments paid a higher price for engaging in malicious cyber-activities"

One threat in cyber-space that few want to talk about is the growing number of state-sponsored cyber attacks on another country's critical infrastructure. These are designed to achieve both military and political objectives and have become increasingly attractive to state agencies and their proxies. This is partly because the culprits are so hard to track down, but with national security and peaceful international relations at risk, it is time governments paid a higher price for engaging in malicious cyber-activities.

Part of the answer is a new international legal agreement which commits signatories to stop directing malicious cyber-activities at infrastructure that is vital to the well-being of civilians, such as telecommunications, finance and energy. Governments will also have to agree to accept responsibility for dealing with malicious cyber-activities originating from, or transiting through, their jurisdictions, rather than claiming either that they know nothing about it, or are not responsible for it.

There needs to be a new international agency to monitor, detect and report on violations of the rules, with the power to put public pressure on states if they fail to act on evidence of malicious behaviour. Some will no doubt say that this is too idealistic, and that legal agreements won't stop such activities. It is certain that states that are confident of their offensive and defensive cyber-capabilities are less likely to support an agreement to limit their options than countries that feel threatened by such attacks. But continued inaction will allow this arms race to intensify, with unpredictable consequences for all who depend on a secure and functioning cyber-space. A new legal agreement would at least provide the world with the capacity to manage this growing menace. ■

Liis Vihul
Legal Analyst, NATO Cooperative Cyber Defence Centre of Excellence

"It is premature to bind states into any new legal instrument when the future of their activities in cyber-space remains so uncertain"

The vexed issue of whether the international community needs a new legal agreement on cyber-security has in recent years turned into a high-level political game. Some nations are strongly in favour of adopting a new global treaty, others are equally opposed. In my view it is premature to bind states into any new legal instrument when the future of their activities in cyber-space remains so uncertain, and while we still don't know how to apply existing laws to current cyber "reality".

The most widely discussed topic among legal experts is how jus ad

bellum (international law governing the use of force) and jus in bello (international humanitarian law) are to be interpreted in the modern cyber context, and the extent to which they apply. To shed light on these questions, the NATO Cooperative Cyber Defence Centre of Excellence is sponsoring the development of the "Manual on International Law Applicable to Cyber Warfare" – or the "Tallinn Manual" for short. Written by a group of top legal experts, it aims to establish an authoritative reference on the subject and is due to be published towards the end of 2012.

But no legal textbook can answer such imponderables as what nation states will be up to in cyber-space in another few years, or what types of international behaviour a new legal instrument would be expected to regulate. Since negotiating a treaty is a lengthy process, and states are still developing their cyber-capabilities and formulating their strategies, any treaty negotiated now could well be out-of-date before the ink is dry. It therefore seems both prudent and wise to adopt the approach of many western nations: to promote rules of behaviour and determine best practices, rather than pressing for a new global treaty. While some states will no doubt continue to promote strict control over cyber-space, and others will prefer the exact opposite, the correct approach probably lies somewhere in between. ■

Peter Ricketts
Former National Security Advisor, UK Cabinet Office

"International treaties are not the answer; co-operation with business is key"

The UK recently ranked cyber-attack as one of the gravest threats to its national security. In response, our national cyber-security strategy set out how the government aims to meet this threat while continuing to seize the economic and social opportunities of the online world. For Britain, international treaties are not the answer; co-operation with business is key.

That is because across Europe the critical infrastructure of cyber-space is largely owned and managed by the private sector. This means governments have to do more than share actionable information on cyber-threats. They have to find innovative ways to become partners with companies to ensure their systems and data are secure. In return, companies have to raise their awareness of threats, and invest more in protecting their systems.

Co-operation with the public is, of course, also necessary. Governments have to help individuals acquire the know-how to protect personal computers and devices. But people also have a responsibility to be careful about the information they put online, as well as making sure they keep their security software updated.

At the international level, the UK does not believe that binding treaties between governments are the answer. They could take decades to negotiate, by which time cyber-space will have changed beyond recognition. A more practical goal is to build an international consensus on "rules of the road" – an agreed set of norms governing behaviour

in cyber-space. This must involve businesses and civil society around the globe as well as governments, since an open, trusted and stable cyber-space is of benefit to us all.

One area where additional government action is required, though, is practical, confidence-building measures between states to avoid the risk of misunderstandings during responses to cyber-incidents. The recent London conference on cyber-space laid the foundations for such an approach, which will be followed up in Hungary this year. ■

Daniel E. Lungren
Member of U.S. House of Representatives

"There is no silver bullet that will solve the problem of cyber-security"

The proper role of government in cyber-security is a matter of much debate on this side of the Atlantic. The U.S. government possesses information and technical capabilities beyond the reach of those in the private sector. So should it be government that provides security for the nation's digital networks? Or should it set new security standards that companies have to achieve on their systems? In my view, the answer to both questions is No.

The internet is now so complex that it would be exceedingly difficult for any one organisation to manage the system, or ensure its integrity, without massive resources and sweeping powers, including the authority to standardise security practices. Such standardisation could, however, restrict the very innovation that created the global IT industry. Official standards could also limit the flexibility, and therefore the value, of private networks. In the long run, standardisation could also make networks more vulnerable to cyber-attacks rather than less, especially in cases of state-sponsored hacking. And we must remember that almost no country has escaped the impact of the global economic downturn, so the introduction of costly new regulations would be poorly received.

For all these reasons I believe it would be a mistake for the U.S. government to try to provide cyber-security or to manage security on national networks. Instead it should enable strong cyber-security by providing companies with the information they need to protect their own systems. The government should share information on threats and risks, and facilitate the exchange of best practices and security techniques within the industry. It should also create an environment in which companies are encouraged to take more than minimal security steps and reward those companies that do so.

There is also at the moment much discussion about moving cyber-security into "the Cloud", essentially by making Internet Service Providers the first layer of defence for both government and private networks. This is an innovative step and will be explored. But since there is no silver bullet that will solve the problem of cyber-security, pushing the responsibility onto ISPs cannot be the entire answer. ■

Jamie Shea
Deputy Assistant Secretary General, Emerging Security Challenges, NATO

"We should not over-hype the cyber-threat"

When I first took on a responsibility for NATO's cyber-defence nearly two years ago, only a handful of allies were aware of the gravity of cyber-attacks. The United States in particular was experiencing increasingly sophisticated attacks against its military command and control systems, defence contractors and high-tech companies. But many saw that as natural in view of the leading role of the U.S. in military, economic and technological domains. Others believed that they could take the risk of nothing, or at least nothing serious, happening to them.

This situation has now changed dramatically. Although only Estonia has so far had its government and banking sector disabled for days on end because of a cyber-attack, all allies have suffered financial losses, the theft of industrial secrets and key networks taken out of service as the result of denial of service or advanced persistent cyber-breaches. If the organisations or companies attacked had an obligation to reveal publicly their losses, the true extent of the cyber problem would be even clearer.

At the recent London conference on cyber-space, estimates of annual profits from cyber-crime went as high as $1 trillion, putting it on a par with the global narcotics trade. Throughout 2011 we have witnessed a string of sometimes spectacular hackings of organisations that one would have thought were relatively secure: Lockheed Martin, Google, the French economics ministry, Sony, the EU External Action Service and, not least of all, NATO. The Dutch company DigiNotar had its security certificates stolen by a single Iranian hacker, compromising the identities of 300,000 Iranian users. Security previously considered effective has been revealed as surprisingly vulnerable to the most skillful or well-resourced cyber-criminals.

At the same time, the ease of access for cyber-criminals suggests that the problem is likely to get worse before it gets better. Malware is developing exponentially. The U.S. security firm Symantec counted 1.5 million new forms last year alone, even if much of this malware can only be used once before a patch is applied. Much malware can be acquired for free, or costs infinitely less than the systems it can attack.

A virus downloaded for $26 on the internet was used to access the video imagery from U.S. drones over Iraq. With so many different actors from every corner of the world able to play in cyber-space – state intelligence services, military establishments, organised crime syndicates, citizens' "hacktivist" groups or disaffected private individuals – cyber will remain for many years to come the ultimate form of asymmetric warfare: easy to attack and hide one's identity, and hard to defend against and identify the attacker.

At the same time, new types of malware have crossed the threshold from the virtual world to the real world of actual physical damage or destruction. The most celebrated example is Stuxnet, which was implanted into the Siemens operating system at an Iranian nuclear plant. Allegedly it destroyed 1,000 centrifuges by making them spin out of control. Stuxnet was able to programme itself, seek out its target and initially hide its traces. It also underlined how even closed systems, delinked from the

internet, can be vulnerable to sabotage, in this instance from a USB stick.

In a similar vein, we should not over-hype the cyber-threat. There is much that we can do to reduce it. For instance, cyber-attacks depend on anonymity. Once we can trace the source of an attack (and we are well on our way to doing so), the credible threat of criminal prosecution or retaliation will go a long way towards restoring deference in cyber-space. Equally we can improve identity authentication and our intrusion detection systems. We can reduce the all-too-easy access to sensitive information following the wake up call of the Wikileaks disclosure. An international code of conduct will eventually emerge to oblige states to co-operate in cyber-investigations and freeze data for evidence.

Finally, we must distinguish between cyber as a problem and over-hyped scenarios like cyber "Pearl Harbors" or a "Cybergeddon". There is no evidence to date that a country can be durably paralysed by cyber-attacks or can lose a war wholly in cyber-space. The internet of the future will be designed increasingly with safety in mind and, once liabilities for cyber-attacks and losses are more clearly established, the key public and private sector actors will have a greater incentive to invest in security. So, cyber-threats are a challenge that we will in time learn to contain, if never totally to control. ■

Giampaolo Di Paola
Italy's Defence Minister

"We need a balanced view that recognises there is a cyber-threat, but neither under-estimates nor over-hypes the problem"

Cyber-space is constantly evolving in tandem with technological progress, a fact that offers great opportunities for developments in the scientific, social, economic and industrial spheres. But this state of flux also creates complications. It means, for example, that the "domain" of cyber-space defies clear definition, despite being part of daily life in most sectors of modern society, including the military.

It also means it has not been possible to bring international discipline to its legitimate uses, despite initiatives in NATO, the EU and the UN. These constant changes mean that many of the threats and vulnerabilities posed by potential cyber-attacks remain unknown.

With digital technology now so deeply embedded in modern society, there are potentially catastrophic scenarios for cyber-attacks. On the other hand, no electronic, communications, information or cyber-system can be made totally safe because of the continual development in the nature of the threat. What is therefore needed is a balanced view that recognises there is a cyber-threat, but neither under-estimates nor over-hypes the problem.

At the same time, we have to be vigilant. The more a society depends on cyber-space, the more it should try to stay up-to-date with technological developments, and be adequately prepared to face any potential threat, either to prevent or at least to mitigate its possible consequences. We have to analyse current threats, assess capabilities and defensive measures, and

find ways, if possible, to reduce or eliminate vulnerabilities.

Is this achievable? Surely it is, but it will require time, human and financial resources and a comprehensive approach, by which I mean a joint, integrated effort by all sectors of society, including civilian, military, industrial and academic, both nationally and internationally.

Getting ready to face these challenges is a must for all states, not only to safeguard their national and international interests but also to give their societies free and safe access to this "global common". ■

Isaac Ben-Israel
Director of Security Studies, Tel-Aviv University and Chairman of Israel's National Council for Research & Development

"Cyber-warfare capabilities will not replace traditional combat methods"

Cyber-attacks against government sites in Israel and elsewhere have become a daily routine. Hackers mostly use primitive but effective techniques simply to overload the communications lines through massive simultaneous attempts to enter into these sites by enslaving innocent computers (Distributed Denial of Service). After one such attack in Estonia in 2007, and the destruction of Iranian uranium enrichment centrifuges in 2011 by the more sophisticated cyber-worm known as Stuxnet, many Western governments became aware of this growing threat and began to set up national cyber-protection.

Cyber-security is a wider concept than information or data security. Computers are embedded in each and every critical infrastructure, whether it be power production, water and food supply, communications or transportation. Penetration of these computers can paralyse those systems and cause physical damage of a sort that until now could only be caused by a military attack. So, a new type of war is emerging, and in this cyber-war a relatively small group of computer experts can paralyse a country without shooting a single bullet or a missile.

Cyber-security is therefore a necessity. The question now is whether it is already more important than traditional defence capabilities, and whether one can shift resources from one to the other.

Unfortunately, the growing capabilities of cyber-warfare and defence will not replace traditional combat methods. This new realm will only provide more innovative tools to be incorporated into future wars, as cyber-warfare is going to be integrated into traditional warfare.

Conventional modern weapons are computer embedded, and there is no way to operate a modern military force effectively without leaning heavily on Command, Control and Communication systems that are all of them controlled by computers. They also are the "brains" of smart bombs and control space assets from the ground. Cyber-technology may harm these systems through the use of computers, and future wars will include brute force attacks as well as "soft" cyber-attacks. The 2008 South Ossetia war between Georgia and Russia showed us that these "soft" blows in cyber-space may prove very painful in the physical space. ■