SDA
SECURITY & DEFENCE AGENDA

Cyber-security:
The vexed question of global rules

An independent report on cyber-preparedness around the world

With the support of McAfee
An Intel Company

About the report

This report is published as part of the Security & Defence Agenda's (SDA) cyber-security initiative. It is intended as a snapshot of current thinking around the world on the policy issues still to be resolved, and will form the basis of SDA debates and future research during 2012.

About the SDA

The SDA is Brussels' only specialist security and defence think-tank. It is wholly independent and this year celebrates its 10th anniversary.

About the author

Brigid Grauman is an independent Brussels-based journalist whose work appears widely in international media like the *Financial Times* and *The Wall Street Journal*. She's currently engaged on a number of projects for institutions, including the European Commission.

Report advisory board

Jeff Moss, Vice-president and Chief Security Officer at ICANN and founder of the Black Hat and DEF CON computer hacker conferences

Reinhard Priebe, Director for Internal Security, Directorate General for Home Affairs, European Commission

Andrea Servida, Deputy Head of the Internet, Network and Information Security Unit, Information Society and Media Directorate General, European Commission

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

Brooks Tigner, Editor and Chief Policy Analyst at Security Europe

My thanks to all those who contributed to this report, both those I have quoted and those I have not. Special thanks to Melissa Hathaway and Jamie Shea for their helpful comments on my draft text, to McAfee's Dave Marcus, Phyllis Schneck and Sal Viveros, and to the SDA's Pauline Massart and Igor Garcia-Tapia.

Contents

Introduction . . . 3

RECOMMENDATIONS . . . 5

PART ONE

Section I. **Clearing the booby traps from the cyber-security minefield** . . . 6
- Terminology: Cyber-war and cyber-attack have many meanings. It's time to settle on just one . . . 6
- Moving into uncharted waters: Cyber-crime pays because it's profitable, low-risk and anonymous . . . 8
- Trust is a most elusive notion: The internet was built on trust, and that's why it's so vulnerable . . . 9

Section II. **Tracking the cyber-revolution: New threats and changing ethics** . . . 10
- Cracking Duqu: The virus admired by experts . . . 11
- Should we be talking of a new ethos? . . . 13
- Smart phones pose security challenges . . . 14
- Cloud computing: The challenges of separating network from content . . . 15

Section III. **Cyber-defence strategies: The hottest debates and conditions for success** . . . 16
- Developing an offensive stance; Cyber-crime and punishment; Protecting an increasingly integrated global system; How safe are SCADA systems?; Net neutrality: Towards international rules; Building a more solid architecture; Tackling weakest-link countries; Securing the supply chain; Increasing awareness of the scale of the problem; Taking a holistic approach; Promoting dialogue between techies and decision-makers; Defining the role of governments; Governments must take greater care when taking advice; Information-sharing at an international level; Thinking differently about cyber-security; Reducing secrecy; Harmonising codes and laws; citizen awareness; Defining pre-emptive cyber-attacks

Section IV. **The quest for rules and regulations to govern cyber-space** . . . 22
- Cyber norms and common security standards . . . 23
- The difficulties of going global . . . 23
- Adapting existing rules . . . 25
- The lack of international mechanisms . . . 26
- The "impossible dream" of a global treaty . . . 26
- A realistic alternative to a peace treaty: Cyber-confidence measures . . . 27
- The bodies competing to govern cyber-space . . . 28
- Internet governance . . . 29
- Standardisation . . . 29
- Law enforcement . . . 29
- Information-sharing . . . 30

Section V. **Breaking down the walls between the cyber-communities** 32
• The generation divide 32
• Improving trust between industry stakeholders 33
• Overcoming the barriers between rivals 33
• Are cyber-crime and cyber-security one and the same? 34
• Steps towards global sharing 34

Section VI. **The private sector's privacy dilemma** 35
• Why the private sector would be better advised to share information 35
• Making regulations that make sense for everyone 36
• The blame game: From software companies to service providers, who should be responsible for what? 37

Section VII. **Bearing the costs of cyber-insecurity** 38
• The insurance sector wakes up 39

Section VIII. **Private citizens : issues of freedom and protection** 42
• Internet responsibility: From private users to corporate giants 43
• The cyber-security skills gap 43

PART TWO
Section I. **A worldwide brainstorming of experts** 45
• Key attitudes 47

Section II. **Country-by-country stress tests** 48

• Australia 51
• Austria 52
• Brazil 53
• Canada 54
• China 55
• Denmark 57
• Estonia 58
• The European Union 59
• Finland 61
• France 62
• Germany 64
• India 65
• Israel 66
• Italy 67
• Japan 68
• Mexico 70
• NATO 71
• The Netherlands . . 72
• Poland 74
• Romania 75
• Russia 76
• Spain 78
• Sweden 79
• United Kingdom . . . 80
• United Nations 82
• United States of America 83

Section III. **Indices and glossaries** 86
• Cyber sources-contributors to this report 86
• Glossary of organisations 94
• Glossary of companies 101

About the Security & Defence Agenda 103

Introduction

This report is made up of a survey of some 250 leading authorities worldwide and of interviews carried out in late 2011 and early 2012 with over 80 cyber-security experts in government, companies, international organisations and academia. It offers a global snapshot of current thinking about the cyber-threat and the measures that should be taken to defend against it, and assesses the way ahead. It is aimed at the influential layperson, and deliberately avoids specialised language.

For the moment, the "bad guys" have the upper hand – whether they are attacking systems for industrial or political espionage reasons, 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 been about dousing the flames, although recently the focus has been shifting towards more assertive self-protection.

The preparation of this report has been greatly helped by Robert Lentz's framework for measuring levels of cyber-security in governments and private companies. Lentz is President and CEO of Cyber Security Strategies, and has 34 years experience working for the U.S. government. His Cyber Security Maturity Model explains the five stages towards resilience against cyber-attack, through conventional threat to advanced persistent threat, and was used as the measurement tool for our country-by-country stress test in the second part of the report.

Even if everyone accepts the need for standards, rules, laws, codes of conduct and maybe even 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 cyber-security is only as good as its weakest link, and that something must be done about unregulated countries that can offer a haven for cyber-criminals.

The first part of this two-part report concentrates on the main issues that are slowing progress, starting with the absence of agreement on what we mean by terms like cyber-war or cyber-attack. It 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 he or she also has a right to privacy and security that should be protected by laws. 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. For these countries, any state has the right to control content within its sovereign internet space.

Linked to the rights and responsibilities of states is the thorny issue of attribution. There are those countries that say that attribution to a specific attacker is impossible, and that the focus has to be defence from attacks. Others argue that attribution is possible, but requires international cooperation, sharing of information and assistance from local authorities.

Some states believe that cooperation 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 arenas; the need for much greater international cooperation; 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 gap-filler until a treaty is agreed.

The second part of this report are 21 country stress tests, complemented by findings from the global survey the SDA conducted in the autumn of 2011 among 250 top cyber-security specialists in 35 countries. They included government ministers, staff at international organisations, leading academics, think-tankers and IT specialists, and their views diverged widely on how to improve international cooperation in cyber-space, which over half of them now consider a global common like the sea or space.

Everyone agrees that cyber-security presents a global rather than a national challenge. But how global should our attempts at a solution be? It would be my hope and that of the SDA that this report will help show where global thinking on cyber-security currently stands, and how to improve it. The following recommendations are a step in that direction. They are not directed at specific bodies or institutions, but are intended as a checklist for achieving international solutions to global regulatory questions.

Brigid Grauman, February, 2012

Recommendations

1. Build trust between industry and government stakeholders by setting up bodies to share information and best practices, like the Common Assurance Maturity Model (CAMM) and the Cloud Security Alliance (CSA).
2. Increase public awareness of how individuals can protect their own internet data, and promote cyber-security education and training.
3. New problems and opportunities created by smart phones and cloud computing must be examined. Cloud computing needs an appropriate architecture to achieve optimum security levels.
4. Prioritise information protection, knowing that no one size fits all. The three key goals that need to be achieved are confidentiality, integration and availability in different doses according to the situation.
5. Consider establishing cyber-confidence building measures as an alternative to a global treaty, or at least as a stopgap measure, knowing that many countries view a treaty as unverifiable, unenforceable and impractical.
6. Improve communication between the various communities, from policy-makers to technological experts to business leaders both at national and international levels.
7. Enhance attribution capabilities by investing in new technologies, and establishing rules and standards.
8. Follow the Dutch model of a third party cyber-exchange for improved private-public partnership on internet security.
9. Despite the many practical hurdles in the way of transparency, both for private companies and for governments, find ways of establishing assurance – or trust – through the use of security mechanisms and processes.
10. Move the ball forward and encourage integration of cyber into existing processes and structures. Make sure cyber considerations and investment are present at every level.

PART ONE

Section I. Clearing the booby traps from the cyber-security minefield

There is little agreement between experts and national authorities on terminology, and without that the prospects for regulating cyber-space are poor

A central feature of the cyber revolution is that no one agrees on the terminology. There's the language of the military and the language of the geeks, and a wide variety of interpretations in between. The place to start any global discussion on cyber-security is therefore to agree common definitions, but so far this hasn't happened.

And yet if we are to set up safety rules in this vast ocean of good and bad, of global inter-connectivity that opens the doors equally to educational opportunity and to global crime, we have to agree on what we are talking about. Do we want to take the more military stance of the U.S., or do we want a consensus in which all stakeholders participate?

Experts compare the need for rules and regulations to those of the road. In the early days of the motor car, the few drivers who took to the road learned as they went along. Nowadays, we snap on our seatbelts almost by instinct. The rules of the road make for safer cars, safer drivers, safer pedestrians. Some argue that the approach to the internet should be similar.

Terminology: Cyber-war and cyber-attacks have many meanings. It's time to settle on just one

The three distinct activities in cyber-space are cyber-espionage, cyber-crime and cyber-war, each with its own motivations and goals. Cyber-war is the most contentious. Former U.S. cyber-security tsar Richard Clarke describes in his book *Cyber War* an American Armageddon of aircraft dropping from the sky and crashing subways. Although not everyone shares this chilling vision of the future, many talk of cyber as a "weapon of mass disruption".

Stewart Baker is clear about what he means by cyber-war. The Steptoe & Johnson partner and former Assistant Secretary of Homeland Security under President George W. Bush says: "The people who pooh-pooh cyber-war do

so mainly by saying that no war takes place in cyber-space only. That's like saying air wars only took place in the air, when air warfare is always part of a larger battle."

According to Baker, in a 21st-century war cyber-weapons might be the first deployed, alone or with other weapons. "It's not unlike air power," he says. "Cyber-weapons allow you to do a bunch of things that leave it a little ambiguous as to whether or not this is a state of war. Are no-fly zones an act of war? Even if it was only moderately effective, the attack against Georgia in 2008 was a cyber-war."

Isaac Ben-Israel, cyber-security adviser to Israeli Prime Minister Benjamin Netanyahu, puts it succinctly. He talks of the specifics that make a cyber-war. "A cyber-war can inflict the same type of damage as a conventional war. If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting a single bullet."

"If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting a single bullet."

Isaac Ben-Israel

Others think we haven't yet seen a cyber-war. **Mohd Noor Amin** is Chairman of the Malaysia-based NGO Impact (International Multilateral Partnership Against Cyber Threats). He puts it differently. "I believe that what happened in Georgia in 2008 was a conventional war with offensive cyber elements. Our view is that we haven't yet seen a pure and significant cyber-war."

Tim Scully, CEO of stratsec and Head of Cyber-Security at BAE Systems Australia, introduces a nuance, and that is to use words prudently so as not to turn cyber-space into a potential battlefield. "The over-use of the terms cyber-war and warfare tends to push the cyber-security problem into the government and defence spheres, thereby potentially ignoring the impact of the cyber-threat on the private sector and creating an imbalance in government funding. I try to avoid the use of the words cyber-war or warfare as they can lead to the militarisation of cyber-space."

Let's think in terms of what we already know to get our minds around it, says **James Lewis**, Director of the Technology and Public Policy programme at the Center for Strategic and International Studies (CSIS) in Washington DC. "It's time to locate thinking about cyber conflict into the framework of existing international law and strategy. The attack against Estonia was not an attack and didn't trigger NATO's Article 5*. It was not a military action."

* Article 5 of NATO's Washington Treaty calls on its member states to collectively defend any NATO nation that is attacked

Moving into uncharted waters: Cyber-crime pays because it's profitable, low-risk and anonymous

Unlike the nuclear threat and others before it, the cyber-threat was upon us with little warning and had a very short gestation period. According to McAfee, every year sees one million new viruses, from worms to logic bombs, and that figure is climbing. The threats come from sources ranging from the criminal (online fraud now dwarfs all other forms of fraud), other states, usually for reasons of espionage, across to politically motivated hacktivists and terrorists who use it mostly for recruitment purposes.

Three factors make cyber-crime so tantalising for criminals. **Costin Raiu**, an anti-virus expert at the Russian security company Kaspersky Lab, says it's a "three-headed hydra." The first is that it's profitable. The second is that it's low-risk. The third and most important is that it's anonymous. Attribution is one of cyber-crime's trickiest problems.

"I try to avoid the use of the words cyber war or warfare as they can lead to the militarisation of cyber-space".

Tim Scully

"The core problem is that the cyber-criminal has greater agility, large funding streams and no legal boundaries to sharing information, and can thus choreograph well-orchestrated attacks into systems," says **Phyllis Schneck**, Chief Technology Officer for Public Sector at McAfee. "The good guys have to attend meetings and publish reports to enable even minimal data sharing to track their opponent. Until we can pool our data and equip our people and machines with intelligence, we are playing chess with only half the pieces."

Now that cyber-space means borders no longer mean anything, countries have to work together as does everyone who claims a stake in it. And that means decision-makers and intelligence services down to the citizen at home on his or her computer or smart phone.

With cyber-attacks, the number of targets is almost limitless. It took some 20 to 30 years after the advent of the nuclear age to put arms control systems in place. We can probably expect the setting up of an international system of cyber-rules and regulations to take time too.

"We're moving into new territory," says **Alastair MacWillson**, Global Managing Director of Accenture's global security practice. "The dynamics of cyber is moving so fast – its intent, its uses and the pace of change. There

are many business models. No one has really got their mind around what all this really means and what we should do about it."

Hype is inevitable with any attack involving trillions of currency losses, although the figure is often pure extrapolation. How do you evaluate the loss of a source code? Or the theft of intellectual property? What are we actually defending? What do we need to protect?

Lars Nicander who heads the Centre for Asymmetric Threat Studies at the Swedish National Defence College believes the main threat is penetration of poorly protected systems. "Stuxnet," he says referring to the computer worm that in 2010 damaged the centrifuges at the Nantaz nuclear plant in Iran, "was more about intelligence gathering. That's what we should be worrying about – qualified terrorists getting access to badly protected information systems. Although you need to be a state actor to do something really difficult."

"In some cases, who cares who did it?," says Canadian expert and practitioner **Rafal Rohozinski**. "We need to arrive at a more graded definition of cyber-attacks. Now we have this universal way of talking about them, which doesn't allow for different definitions of culpability. Sometimes we just want to know what jurisdiction to hold responsible."

Trust is a most elusive notion: The internet was built on trust, and that's why it's so vulnerable

As Israeli security adviser **Isaac Ben-Israel** says, the most vulnerable target for cyber-attacks is a country's critical infrastructures – power, water, telecommunications, transport, hospitals, banks. In most countries, these assets are in private hands, so the challenge now is to develop a strong enough private-public partnership to secure these systems, and to convince people to make that investment. Anticipation is often seen as a waste of money.

The internet was famously built on trust, with few safeguards to protect it. Early-day hackers attacked systems for the challenge they posed. Now it's about making money and stealing intellectual property and military and industrial secrets. But trust is still very much the operative word.

Some people call it "assurance". What are the safeguards we need to put up to make sure we can trust the systems we use daily? Should software companies be held liable for their products? Should internet service providers? How can we make sure the components in the entire IT chain are trustworthy? Does cloud computing give rise to insoluble issues of jurisdiction? Should we be creating international agreements to establish who takes responsibility for sovereign cyber-space? Good brains around the world are thinking about these issues. Not everyone shares the same views, but most know that the internet is here to stay and that it's a global – not a national – issue.

Section II. Tracking the cyber-revolution: New threats and changing ethics

Time for a change of mindset

How dangerous is the cyber-threat? Are we more vulnerable now, or are we developing promising new defensive technologies?

The near-unanimous perception is that we are more vulnerable than before. The number of systems coming on line is growing exponentially, and our reliance on technologies increases daily. Last year, internet pioneer Vint Cerf famously suggested that we do a massive reboot and start all over again in a more regulated environment, but most people think that's pie-in-the-sky.

"Are we becoming part of a totally unregulated data revolution?" asks UK information and security lecturer **Christopher Richardson**. Richardson doesn't think the picture is as dramatic as some people paint. "There's a big degree of hype. We don't know what's really happening." He suggests that we are given a skewed idea of how many incidents really occur, both in the public and private sectors because of secrecy concerns. He notes how few of the many students he teaches every year have so far been attacked.

"You have this perception from the papers that everything is growing worse and worse," says **Olivier Caleff**, Senior Security Consultant at the consultancy Devoteam, "but it's not very different from what we had before. More people are connected, more people are trying to get around security systems, more people are involved in security, we have more tools to detect issues. We have more of everything, including knowledge."

Whatever the hype, the rise in cyber-crime is inevitably going to see more rules, laws and limitations on how people can use the internet. What 40 years ago was a gentlemen's group of users is now a lucrative and low-effort playing-field for cyber-criminals. "The internet allows anyone to send anything anywhere and it will likely get there," says **Phyllis Schneck** of McAfee. "We must destroy the profit element by improving our control over the routing, delivery and execution of malicious instructions, and block the threat. Swimming pools have chemical filters. Networks and computers need intelligence filters to prevent enemy instructions from finding their target."

"Swimming pools have chemical filters. Networks and computers need intelligence filters."

Phyllis Schneck

Another problem is that the introduction of new technologies brings unforeseen causes and effects. When researchers defined the protocol behind the email system, they didn't consider spam was a threat because it cost too much to send an email. "But technology evolved and spam took over because of a weakness in the original protocol," says leading Danish expert **Christian Wernberg-Tougaard**. "That's been one of the catches of the IT industry for a number of years. We need to consider carefully how to implement new technology."

Wernberg-Tougaard recommends that the "better minds" in the public and private sectors get together with researchers to discuss the impact of today's technology on tomorrow's world.

For men like **Richard Crowell**, professor at the U.S. Naval War College in Newport, Rhode Island, we need to think cool-headedly about the new domain the cyber-threat represents to understand the new risks. "We're at the same point we were in the inter-war years," he says. "The (WWI) battle of Gallipoli was a big failure for the Allies and it taught us never to do amphibious warfare again. We had to successfully learn to move from one domain to another, from sea to land. That's what the thinking was all about at service colleges in the 1930s and 40s. And we've reached that stage again."

"We're thinking increasingly about boundaries and protecting our own information better," says Crowell. But he concedes that after 30 years in the Navy through the Cold War, he has a mindset that is radically different from his son's. "My son's idea of access to information is much more open that mine. I think young people need to think more about what they post on the internet, and my generation needs to think more openly."

Cracking Duqu, the virus admired by experts

At the time of writing in early 2012, the mother of all Trojans is called Duqu. That is until the next one turns up. For many people like **Costin Raiu**, global director for Research and Analysis at the Russian security company Kaspersky Lab, this was by far the most exciting attack of his career.

For several months, Kaspersky Lab and security software company Symantec have been studying Duqu to try to understand how the virus operated

undetected for four years. "Understanding it will allow us to design the data security technologies of the future," says Raiu.

"Young people need to think more about what they post on the internet, and my generation needs to think more openly".

Richard Crowell

What has Duqu taught Raiu?

Among other things, that the Duqu and Stuxnet worms were invented by the same software company, and that they struck far and wide infiltrating computers in France, the UK, Taiwan, Germany, South Africa, and elsewhere. "We suspect," says Raiu, "that Stuxnet's focused attack on the nuclear centrifuges in Iran was done thanks to information previously stolen by Duqu."

Raiu greatly admires the skills involved. "Duqu used exciting technologies in brand new ways. Most Trojans steal information and send it on. With Duqu, every action is split into so many components that you can't tell this

THE CYBER-SECURITY VENDOR'S VIEW

David Marcus is Director of Advanced Research and Threat Intelligence at McAfee Labs, and writes his own blog. He's not so much interested in what's next after Duqu as curious as to its long-term potential repercussions. "The unique thing about Duqu is that it potentially targeted certificate authorities, and used stolen and forged certificates to create rogues that became whitelisted drivers. How is this potential in the attack going to evolve?" he asks.

McAfee's work, he says, gives him a vendor-specific way of looking at the universe. It's all about protecting customers' data and assets and ensuring safe communications, and about preventing bad things from happening.

From his perspective, cyber-spies and cyber-criminals are in many ways much the same. "They may use exactly the same tools and techniques. Sometimes, the same attack can have both cyber-crime and cyber-espionage goals. Often, they differ only in how they intend to use the stolen data or IP."

Although Marcus recognises that smart phones and cloud computing raise issues of sovereignty, responsibility and ownership, he says they don't

is a malicious attack. When you bring the components together, then it obviously is."

For Kaspersky and other anti-virus labs, the challenge now is to create protection against similar technologies – taken apart, they seem innocent, but put together they are very dangerous.

Should we be talking of a new ethos?

Everyone agrees that galloping changes in cyber-space don't mean the system has reached maturity. "An immense set of changes is on the way," says CSIS expert **James Lewis**, "and that includes how to play out the extension of sovereignty, changes in governance and perhaps even reconsider our kind of freewheeling approach to the internet."

Laws and international agreements are key, says Sweden's **Lars Nicander**. "To take one example; when Estonia turned to Russia for legal assistance during the 2007 cyber-attacks, Russia declined to help because they hadn't signed an agreement to protect critical infrastructure. We have to expand governance systems."

For **John Meakin**, Chief Security Information Officer at oil giant BP, "there is no question that from where I am sitting at BP the advent of new technologies represent a truly new threat. They are evolutionary rather than revolutionary. "It's the same types of threat thrown at an evolving technology. The problem is nobody is going to want to own responsibility for the data because it's spread out geographically."

A self-styled "connectivity libertarian", he says he struggles every day with the question of defining success conditions for good global cyber-security. "I'm a fan of self-policy," he says, "but I realise the limitations of business and users regulating themselves." In the meantime, he can't see any country that has got its cyber-security act under control. "We are a collection of weak-link countries," he says.

One major problem is that too many companies, enterprises and governments are "busy figuring out technology from a year and a half ago. Technology develops before business gets a handle on it." He isn't convinced government has the right perspective because most politicians and elected officials have such a limited understanding of technology, often due to their age. "They are not techies," he says. "They have no idea how quickly technology changes, how volatile it is. At least the younger generation has an implicit understanding of how fast information changes hands, the nature of changing data."

is causing us to change our security model. The old model of internet security basically said, 'It's secure because we own it.' Whereas now the challenge is how do we keep it secure when we don't own the internet? We may own the data but we don't own the internet. When we don't own the data's container, what happens? That's really it in a nutshell in terms of changing ethos."

The new thinking in the IT security community is that new firewalls, new encryption algorithms and so forth, are not enough to make people feel safe. "So far in Europe, America and Asia, we've been focussing on the mechanisms required to protect the new internet environment," says **Jesus Luna**, who leads a security research group at the Technical University of Darmstadt in Germany, "but we've started to realise that we also need assurance about those mechanisms."

Assurance is about establishing metrics and measurements to generate trust in protective mechanisms. "For instance, you pay your ISP (internet service provider) for its services, but how can you be sure that the ISP's security mechanisms are protecting you against malware or any other cyber-threat? How can you be sure they are providing the right assurance levels?" Luna asks.

Among other such groups, the Common Assurance Maturity Model (CAMM) and the Cloud Security Alliance (CSA) that count Google and McAfee among its members, are working on technology and techniques that give this assurance. CAMM offers guidance on how much to invest in security by using metrics, or the "economics of security". Says Luna: 'We – the academics – have been developing the security metrics that will give this assurance."

Smart phones pose security challenges

Developments like smart phones and cloud computing mean we are seeing a whole new set of problems linked to inter-connectivity and sovereignty that require new regulations and new thinking. Experts talk of the internet of things and services, and things are smart phones, androids (mobile operating systems), tablets and sensors, and services including the cloud.

"The mobile internet is changing things," says Canadian expert **Rafal Rohozinski**. "The next two billion users will be connecting from mobile devices, and many of those devices are in developing countries. The sheer numbers are likely to have social impacts like flash mobs. A lot more politics is migrating to cyber-space, with parallel calls to regulate cyber-space. The governance of the internet as a whole is reinvesting states with the authority to regulate cyber-space."

The issue is also about security and privacy. A smart city - one with sensors on traffic lights, sensors in cars, electric smart grids, patients wearing sensors –

raises many new problems. "What is personal information and how are we going to protect the data in these devices? Are these devices really giving us the right security and privacy levels?" Luna asks.

"We're talking again about assurance," says Luna. "We need a lot more legislation. We need to push companies to enforce data protection mechanisms that protect the privacy of citizens. The EU is doing quite good work on this. This is going to take some time but the early steps are being taken."

Cloud computing: The challenges of separating network from content

As for cloud computing, outsourcing the filing of data has been around for 40 years. What's new is the geographical spread of this storage. The National Institute of Standards and Technology (NIST) provides the standard definition for cloud computing: a rapid, on-demand network access to a shared pool of computing resources. These are not in the stratosphere; they are basically hangars full of servers.

Outsourcing means considerable cost savings, and many companies are now using it for computation and data storage. Bandwidths are now large enough to transfer large amounts of data to data storage facilities. Amazon, eBay, Google, Facebook and all the big names are outsourcing computation to cloud.

"Cloud computing means separating the network from content in ways that didn't exist before".

Rafal Rohozinski

"Cloud computing means separating the network from content in ways that didn't exist before," says Rohozinski. "The laws we have governing copyright and territorial security get skewed." Among other issues raised by cloud computing is the cost of processing power and connectivity and the whole issue of net neutrality. But Luna warns that these new storage facilities give rise to problems of security and jurisdiction. "Who are you going to sue if there's a problem?"

Google, for instance, keeps one third of its cloud in Canada. "Is that information subject to U.S. or Canadian law?" asks Rohozinski. Cloud computing creates new questions for the lawyers. "What does it mean from a liability point of view? How does one handle different data retention and privacy laws? What happens when data shifts location? Who determines the final resting place of jurisdiction?"

Section III. Cyber-defence strategies: The hottest debates and conditions for success

What are now the hottest debates in cyber-space defence strategies? Twenty themes emerged from the interviews conducted for this report

1. Developing an offensive stance

Several countries are formulating plans to respond more aggressively to cyber-attacks, and are making investments in this direction. The UK's new cyber-strategy released in late 2011 brings up the notion of self-defence. This more bellicose stance applies both in the military and private arenas.

William Beer, Director of Information and Cyber-security Practice at PwC, refers to the UK's White Paper of September 2011 that suggests companies should be more vocal and use legal means to protect their organisations. "For instance, instead of writing off losses, they should invest into actively targeting those organisations that have been attacking them," he says. "The old approach was 'I won't tell people.' Now the attitude is 'I'll use every legal means at my disposal to protect my company.'"

2. Rating countries' offensive capabilities

"Everybody only discusses offensive cyber-strategy via veiled references to the Russians and the Chinese without any strong, public, quantifiable proof," says **David Marcus**, Director of Advance Research and Threat Intelligence at McAfee Labs. "No one has stepped back and said, let's take the 30 or so countries we think have offensive cyber capabilities and grade what they are and how they differ." He believes we need a country-by-country rating methodology for offensive capabilities as well as defensive, and says most cyber-security professionals pretty much know what most countries are capable of doing- "It's the countries that have cyber-offensive training programmes at a military or government level, it's those that consider cyber as part of the war theatre."

Marcus believes there can't be strong a defence without a solid, quantified knowledge of offensive capabilities, and that most governments have

developed or are developing cyber-tools and attack tools. "We dance around this issue but is there really any difference between developing fighters and cyber-weapons if they are both used in warfare? Everyone blames the Chinese for everything today, but if we're going to push for government regulations and policy then let's lay out who we think has the top cyber capabilities. I doubt you could find a country that is not working on it."

3. Protecting an increasingly integrated global system

We are looking at an increasingly integrated cyber-world with much more system-sharing and cross-border services, such as cloud computing, and we need the system to be functional and safe wherever it is located.

"How do we protect our infrastructure?" asks Danish security expert **Christian Wernberg-Tougaard**. "It's great to have shared service and cloud," he says, "but how do we protect this multi-faceted structure?"

If a component were to be attacked, or if a country were to become unstable, you might face a serious challenge. The discussion between the EU and the U.S. right now asks such questions as, can you have cloud services within the domain of the U.S. Patriot Act while also being under the EU's data protection act?

4. How safe are SCADA systems?

SCADA systems, known as Supervisory Control and Data Acquisition Systems in the U.S., have always been around. They are the physical elements that control pumps and barrels, and other infrastructural and industrial processes. The challenge is that they used to be isolated systems and now they are often connected to the internet or accessible using data transfer devices like USB sticks. Increasing connectivity means more vulnerability.

"If you can control a SCADA system, you control the facility or the industry," says **Bart Smedts**, Senior Captain and Research Fellow at Belgium's Royal Higher Institute for Defence. "Via SCADA, you can control the economic work of any nation. Once you realise you have a virus on a SCADA system or the internet you can expect it to spread like an epidemic."

"Many of these systems are unprepared for cyber attacks," says **Frank Asbeck**, Counsellor for Security and Space Policy at the European External Action Service. "A lot of damage can be done through ignorance, carelessness or malicious intent." Like other experts, he believes we need to think hard about how these new factors affect systems physically and technically, and then decide what to do about it.

5. Security versus privacy

The issue is whether network data like IP addresses is considered private. Cyber-security providers need to track malware using these IP addresses if they are to block attacks, which is very different from those who collect the same data for marketing or behaviour tracking purposes. "In fact, if cyber-security providers and network providers can use IP addresses to track malware, we believe that more data will be kept private," says McAfee's **Phyllis Schneck**, "because we will be more successful at preventing the bad guys from computer intrusion and unauthorised access to personal information, financial data, intellectual property, and systems that control and monitor physical infrastructure."

6. Net neutrality

The heated debate over net neutrality is about whether broadband providers should be allowed to exert a veto on applications that use large amounts of bandwidth or discriminate among content providers. Brazil and Argentina, among others, are moving forward with net neutrality and opening their market to everyone. In the U.S., the argument is sharply divided; President Barack Obama is a believer in it. "Industries are completely against it," says **Melissa Hathaway**, who runs the consultancy Hathaway Global Strategies and was formerly cyber-advisor to the Department of Homeland Security. "I myself don't think that net neutrality is a good idea," she says. "Industry needs to be that frontline of defence. ISPs, the conduit for delivering content, should be responsible for not delivering some content."

7. Towards international rules

With the increasing threat of states engaging in malicious cyber activities against the critical infrastructure of other states, the need for international cooperation grows daily more urgent. "We need to prepare the battlefield," says **Vytautas Butrimas**, Chief Cyber-Security Advisor at Lithuania's Ministry of Defence. "There are holes in the systems. We need to reduce the risk of another state placing something like a logic bomb that would cause systems to shut down. There is no such thing as zero risk but we can make the risk acceptable."

8. Building a more solid cyber architecture

"We are closing the stable door after the horse has bolted," according to **Christopher Richardson**, lecturer for the UK Ministry of Defence. The current ad hoc approach to regulation isn't going to make the cyber environment a safe place to do business. "There are too many people with too many views," he says. "We need to look beyond particular attacks and improve assurance." Experts talk of improving asset management so as to know what we are trying to defend and creating a "patched up" environment. "We don't need to be scared but educated," says Richardson.

New technology is now focused below the operating system. It communicates directly with the computer hardware and chips to recognise malicious behaviour and be smart enough not to allow it. "The buck stops here," says McAfee's **Phyllis Schneck**. "This is the newest and deepest layer and, together with more intelligence in the other layers, a key part of the future of cyber-security. Communication with the hardware is the queen of the chessboard - it can stop the enemy almost immediately or control a longer game. Either way, we win."

9. Tackling weakest-link countries

"The challenge in the digital economy is that no chain is stronger than its weakest link," says **Christian Wernberg-Tougaard** of the Danish Council for Greater IT Security.

Weakest link countries are those where absence of legislation creates havens for cyber-criminals. One view is to take the drastic option of disconnecting them from the internet. Another is to use tools to filter out internet providers from that country. A number of companies in the U.S. block all Internet Protocol (IP) from China.

"The best solution," says **Costin Riau**, director for Research and Analysis at Kaspersky Lab, "is to try to improve the economic situation in those countries. Internet crime is always connected to unemployment rates."

10. Securing the Internet supply chain

A new discussion centres on the issue of securing the internet supply chain, particularly in sensitive areas of government that form part of the critical national infrastructure. This is about where you get your hardware devices, rooters, servers, switches and so on. Could malware be introduced during manufacturing? Will companies want to work only with certain countries? **Alastair MacWillson** of Accenture says: "This can be seen as a form of protectionism, but it may also be about prudent security mechanisms."

11. Increasing awareness of the scale of the problem

We need greater awareness at all levels and in all sectors, and more dialogue all around. "It's not going to happen overnight but we need much tighter private-public collaboration across borders and across cultures." Says **William Beer**, director information and security practice, PwC.

12. Taking a holistic approach

Hamadoun Touré, Secretary General of the International Telecommunication Union (ITU), is adamant. "As long as we carry on thinking that the solution is only technical we won't get anywhere. We need a holistic approach involving

legal, regulatory and technical measures, as well as an ethical approach. We also need an Integrated Supply Network within an international framework."

13. Defining the role of governments

The view from industry is that there are things that governments can and should do to improve the overall state of security, and things they shouldn't and cannot do. "Governments should be involved in commonality over borders," says **John Meakin**, head of cyber-security at BP, "but they don't have a role to play in the detailed disposition of security mechanisms around any one enterprise's internet estate."

14. Governments must take greater care when taking advice

Who is advising governments? According to BP's Meakin, key decision-making forums are populated with career civil servants, particularly in the U.S. and the UK. Meakin and others like him believe that dialogue at the top needs more experts from the 'buying' side of the industry, as well as its selling side.

15. Information-sharing at an international level

There is no single international agency or body with the mandate to deal with cyber-security. Also, national and regional organisations have to improve cooperation. "Security is so vast that there is a long way to go before we reach trust," says Italian cyber-expert **Stefano Trumpy**.

"We need more and more information sharing," says Japan's **Suguru Yamaguchi**, a leading specialist on network security systems. "That's the difficult part. Global companies are good at sharing information. They could act as catalysts to encourage governments to be more open."

16. Thinking differently about cyber-security

Cyber-security advocates like Australian **Tim Scully** argue that we are wrong to protect our inter-connected systems at the expense of the information they contain. "Right now, our model is systems-centric," he says. "Private and public organisations are being attacked and large amounts of data are being stolen despite traditional boundary defensive measures, like firewalls, anti-virus and intrusion prevention and detection applications." He argues that we should think in terms of trophy information. "People need to focus on protecting their most sensitive information rather than the system itself," he says. "Subsequent segregation of data might even mean that some information is air-gapped from the internet if its loss were to have catastrophic consequences."

17. Citizen awareness

There has to be more widespread awareness that cyber-security starts with everyone's behaviour and awareness. Far too many people at all levels of the hierarchy haven't realised that they should take responsibility for their home computers and the IT system at work. It's a battle that will never be entirely won. "There will always be someone to click on a link they should not click on," says Scully. "Hackers exploit social vulnerability, that is why spear-phishing is so successful."

18. Reducing secrecy

Over-classification of data skews the picture of what is going on. "Secrecy concerns are the bane of cyber-security," says Austrian **Alexander Klimburg**, analyst with the Austrian Institute for International Affairs. "We should put more stock in non-state attribution, security trust networks outside government, to attribute cyber-attacks."

19. Harmonising codes and laws

Discrepancies between code and laws can lead to abuse and should be resolved. **Florian Walther**, senior IT security consultant at Curesec, says this is what happened in Germany when the intelligence services were found to be using spyware in a more intrusive way than spelled by law. "The code defined what it could do and what police forces could do, but the law didn't," says Walther. "The program was making the law, and defining what was and was not possible."

Cyber-attacks can often be seen within network flow patterns, much as storms can be seen forming on a weather radar map, says McAfee's **Phyllis Schneck**. "The collection and correlation of cyber-data requires international agreement," she says, "and it's urgent because the bad guys at present have the advantage. Without these agreements, their behaviour is not always seen in time to thwart an attack."

20. Defining pre-emptive cyber-attacks

Another difficult question is how to define pre-emptive cyber-attacks. What are they? How would you come up with the evidence? How strong can retaliation be? What is proportionate? "Furthermore, you can't attack if you haven't first penetrated the system," says **Jamie Shea**, NATO's Deputy Assistant Secretary General for Emerging Security Challenges. "It's a game of mirrors, like the Menin Ridge at Messines in 1917. Where is the line between defence and aggression?"

Section IV. The quest for rules and regulations to govern cyber-space

It has taken the spectacular increase in cyber-attacks for political leaders in the United States, the European Union and parts of Asia to sit up and take stock of the costs involved and the loss in competitive positions.

"I've been working in computer security for 23 years," says BP's Chief Information Security Officer **John Meakin**, "and it's really only in the last two or three years that policy-makers have begun to wake up."

On the other hand, "If the internet had started with security and control in mind it would never have taken off," says **Alastair MacWillson**, Accenture's global managing partner of global security. "One of its strength is that it is unregulated. It's not in anybody's interest to regulate."

He recalls his concern when U.S. President George W. Bush wanted the authority to regulate and monitor the internet under the Patriot Act. "However," he adds, "companies that use the internet should be much more sensitive to the fact that it's an open highway. They need to invest in the technology that ensures they know who they are doing business with."

As the medium matures, the need for global rules has grown and there are now some 20 political groups and economic forums worldwide addressing cyber-security issues.

Improving corporate governance could solve a number of problems. **Christopher Richardson** who lectures at the UK's Defence College of Communications and Information Systems (DCCIS), thinks that many companies hold on to data they don't need and that strong internal audits should put a stop to this. "We need to look at how we regulate data management and protection everywhere," he says. Encrypting large amounts of data doesn't make sense. "We want smaller units of data and only what is necessary. Why were Sony recording CVV codes on credit cards?"

How else can we make things safer? Establishing market best practices is a good first step that is both practical and low-cost, and can be implemented quickly. In the EU, the mission of ENISA, the European Network and Information Security Agency, includes sharing this kind of information between the 27 member states.

Cyber norms and common security standards

ENISA also works at the complex task of defining standards. "Different EU member states are at different stages," says the head of the technical department **Steve Purser**. "A lot of our work is first seeing how countries deal with things, then defining common standards."

How do you ensure that these standards are observed? "You can either impose them or let the market sort things out. Many organisations now use the ISO 9000 standard; if you have that label you have credibility. We can do the same with the security market."

The way to go, says researcher **Jesus Luna** of the DEEDS security research group in Germany, is to encourage industrial and academic consortia, interest groups and specialised communities, to set up de facto standards that sooner or later will become widely accepted. The cloud security alliance CAMM (Common Assurance Maturity Model) is one such instance. "Fortunately, some private companies realise that working with competitors can benefit them," says Luna. Having international standards is an economic necessity; we need technology that is inter-operable between countries.

The difficulties of going global

National sovereignty is one thing, but in cyber-space collective responsibility can't be avoided. Countries around the world have set up national CERTs, or are in the process of doing so. Large companies and public institutions have also set up these rapid response teams to act in emergencies and inform citizens about computer security, and they are also increasingly taking part in global networks of CERTs.

"If you want to shut down a botnet, you'll be lucky if it's in your own country," says Purser. "International collaboration is essential. Security within national boundaries doesn't make sense. Everything is globally connected. A European approach doesn't make sense unless aligned to the approach of international partners."

But opinions about how to legislate vary. There are those who argue that the internet is changing so fast that regulations will never keep up, others who believe legislation stifles creativity, and countries that want to exert control over content. Is it unrealistic to expect global rules for cyber-security and cyber-privacy?

Probably, says **Stewart Baker**, who worked for Homeland Security and is now a partner in the law firm Steptoe & Johnson. "There's too much advantage in breaking those rules." He is hostile to the EU's data protection directive, aimed at regulating the processing of personal data, calling it an attempt at a "neo-colonial imposition of privacy notions on the rest of the world."

The rift between the U.S. and the EU on the protection of privacy is one bone of contention but there are others. "We should strive for global rules," says **Tim Scully**, CEO of Stratsec and Head of Cyber-Security at BAE Systems Australia, "though they will be difficult to achieve." Like many, he thinks it would be much easier to start with global standards that protect information and to train and certify cyber-security professionals.

Jaan Priisalu, who heads the Estonian Information Systems Authority, thinks we won't get anywhere until the political and the technological worlds understand what the other is saying. "I see huge misunderstandings in every country," he says. "The technological people's culture is how to use the network efficiently and they usually don't like to talk. At the same time, you hear politicians making stupid and arrogant statements about applying and regulating the law."

"We need rules and agreements to keep the cyber world running," says **Kamlesh Bajaj**, Chief Security Officer at India's Data Security Council. "The problem is when policy-makers start to regulate without understanding the issues." For Bajaj, these issues are not solely about compliance. "The challenges posed by the movement of data mean that stringent compliance regulations aren't enough. You might apply them in one country and put your own country at a disadvantage. We need to look at all sides of the argument."

IMPACT, THE CYBER-TALK PLATFORM

With the fast spread of smart phones, including in the least developed countries, cyber-security is in the process of shifting east and south of the globe. Conventional wisdom dictated that cyber-security focus on the richer countries. That view is changing. If we are to avoid safe havens for criminals in countries with no cyber-laws, we urgently need to help those countries.

Mohd Noor Amin, head of IMPACT, the cyber-security alliance headquartered in Malaysia, says "even the most sophisticated countries now realise you have to assist the poorer ones." The ITU-backed platform has 137 member nations and brings together governments, academia, industry and international organisations from developed, developing and the least developed countries.

Adapting existing rules

Do the experts think many rules are already here waiting to be adapted?

Some do. In many cases, it might be simpler to extend the scope of existing laws than to rewrite criminal codes from scratch and design new legislation, they say. "It doesn't take that much of an adaptation of existing criminal codes to take effective action against cyber-criminals," says BP's **John Meakin**. "The problem is that players on the law enforcement side, prosecutors and judges are often ignorant of the way computer systems work."

If we look at international treaties like the Geneva Convention, many existing rules of war may also apply to cyber-space. "There are those who say cyber-space is the fifth dimension of warfare," says Australian **Tim Scully**. "In that regard, I'm sure lawyers could go through some of the existing rules and apply them at an international level to cyber-space."

The thorny issue of attribution may appear to get in the way. Not so, says **Vytautas Butrimas**, Lithuania's Cyber-Security adviser at the Ministry of Defence. "It may be too difficult to track down the computer to the very apartment, the very building, the very person who is pressing the enter the key, but it is technically possible to pinpoint the country where the attack originated."

His view, shared by many, is that we need an international agreement that makes every country responsible for its sovereign cyber-space and thus forced to take such steps as blocking infected computers from the internet. "You'd act in the same way with a cholera pandemic," he says. "The attribution debate also has its calculating and cynical side. States that want to keep their options open when seeking to achieve a political or military objective are opposed to any restraint on their use of cyber-weapons."

"We are not a treaty, but a voluntary cooperation platform," says Amin. "We tackle cooperation issues between countries in different jurisdictions. That cooperation is going to get stronger. Nobody wants cyber-crime to operate in their jurisdiction. The problem is not that nothing is being done, but that those governments with cyber-criminals working in their territory don't know what is going on."

IMPACT runs an electronic platform jointly with the ITU involving law enforcement, ISPs, telecoms regulators and policy-makers. Amin believes that successful information-sharing among IMPACT members will not replace the benefits of an international treaty. "It's a significant first step to getting people around the table. If business competitors can sit at the same table to do something good for the world, why can't governments? A treaty would enhance levels of cooperation."

The lack of international mechanisms

For the time being, there are no international mechanisms that coordinate national cyber-defences, including intelligence gathering. According to Canadian expert **Rafal Rohozinski**, the best coordination and expertise sharing so far is between the Five Eyes – Canada, the U.S., the UK, Australia and New Zealand. "The concentric circles around that are tenuous," he says. "They include NATO, the Council of Europe, and the Collective Security Treaty Organization (CSTO)."

Colonel **Emilio Sanchez De Rojas**, who heads the Department of Strategy and International Relations at Spain's Ministry of Defence, argues for a comprehensive approach that would include all the main actors and organisations – the UN, the Organisation for Security and Cooperation in Europe (OSCE), the EU and NATO, as well as multinational businesses dealing with cyber-security. "But," he stresses, "these rules have to be accepted not only by main powers like China and Russia, but also by more cyber aggressive countries like Nigeria and others in Africa. We need to reach a compromise between security and freedom."

Japan's **Suguru Yamaguchi**, former advisor on Information Security to the Cabinet of the Government of Japan and a professor at Nara Institute of Science and Technology, believes a small first step is the Budapest Convention, the Council of Europe's convention on cyber-crime, the first international treaty to seek to address internet crime, which has been ratified by Japan, the U.S. and China, among 117 other countries. "We are encouraging more countries to sign the treaty," Yamaguchi says, "because it offers a comprehensive framework for capability and collaborations in investigating cyber-crime. State-sponsored attacks are a criminal activity and require the same cyber-security measures."

The "impossible dream" of a global treaty

In 2010 before the UN's ITU (International Telecommunications Union) conference in Mexico, Secretary General **Hamadoun Touré** said he wanted a "cyber peace treaty." But for many, simply agreeing on common rules and setting up a global body are a big enough challenge.

For the more hawkish, like U.S. lawyer **Stewart Baker**, an international treaty is a waste of time. "At worst, it will delude western countries into thinking they have some protection against tactics that have been unilaterally abandoned by other treaty signatories," he says.

The London Conference on Cyber-space in November 2011 wanted to be the launching pad for an agreement on designing a cyber-security treaty, but that was not to be. Too many countries didn't share the same viewpoint. "I'm a realist,' says **Erik Frinking**, who works for the Centre of Strategic Studies (HCSS) in The Hague, "and so I seriously doubt we can have a

global legal agreement. Codes of conduct are already a source of conflicts with the Russians, Chinese and others."

Where cyber-conflict raises its ugly head, Frinking believes we should use the same rules of engagements as for conventional war. "Rules of engagement can be agreed at a very abstract level, but it's hard to see countries agree at this moment on rules applying to other domains." A number of challenges can be handled informally.

"I seriously doubt we can have a global legal agreement. Codes of conduct are already a source of conflicts with the Russians, Chinese and others".

Erik Frinking

If we see cyber-security as a network of safe countries, says Baker, we should think in terms of a rough working consensus that turns outliers into pariahs. "We used to have that problem with banking. A number of money-laundering centres saw opportunities to profit from not enforcing money-laundering rules," he says. "The bigger financial participants in the global financial system shunned these countries pretty effectively, reducing the number of places where you can hide money. Similar mechanism could be applied to isolate countries that don't respond to investigative requests."

"Cyber is a dangerous space," says the ITU's Touré, "and we must create a framework of cooperation to protect basic human rights. Governments have to commit themselves not to attack one another, and we must set up a framework cooperation to arrest criminals wherever they are. Are we ready for such a negotiation? We don't have a choice; we've got to do it for the safety of our children, our businesses and our countries."

A realistic alternative to a peace treaty: Cyber-confidence measures

A number of scholars, including **James Lewis** of the CSIS, Paul Cornish, professor of International Security at the University of Bath, and Theresa Hitchens, Director of the UN Institute for Disarmament Research (UNIDIR), have been working on designing cyber-confidence measures. "A treaty isn't going to work," says Lewis. "There are too many verification, compliance and definitional problems."

Cyber-confidence building measures include, "agreeing on norms to structure expectations about state behaviour," says Lewis. "You want transparency, particularly for national doctrine on how to use cyber-attacks in a military context. Most countries have these doctrines but don't talk about them."

Among other things, CBMs include law enforcement cooperation against the use of proxy forces. "The Russians and the Chinese use proxies," says Lewis, "citizens acting at the behest of government. A traditional arms control treaty that restricts technology won't work because the weapons are sometimes teenagers with laptops. How can you set up a treaty in this context?" The measures would include such commitments as sharing information on third party threats, and taking responsibility for activities of individuals resident in your own territory. Cyber-confidence measures are currently being discussed at the OECD and the UN.

Lewis is scathing about the autumn 2011 London Conference on Cyber-Space. "A giant missed opportunity," as he puts it. With follow-ups in Budapest in 2012 and in South Korea the year after, he hopes lessons will have been learned in what he sees as a serious problem of narrative and understanding of the issues. "People have to stop saying that a free and open internet produces wealth. The development agenda is a flawed concept. China is not free and it seems to be doing just fine." As he sees it, London "danced gingerly around values," and avoided the argument as to why a secure internet based on democratic values serves all countries' interests. "That was the proverbial elephant in the room everyone tried to ignore."

The bodies competing to govern cyber-space

The internet is a messy playing field, run by a patchwork of organisations, and different countries have different views about who should be in charge. Do we want more government control? Or do we want to avoid that at all cost? Or do we simply want to see governments get something moving? And how do we follow a bouncing ball?

The big-picture policy is principally in the hands of the EU, NATO, the UN and APEC, the Asia-Pacific Economic Cooperation. Every year, the UN's Internet governance Forum (IGF) offers a multi-stakeholders' talking shop. It's a lively and democratic Babel's Tower. In the cacophony of nations, India, Brazil and South Africa have called for a new global body to control the internet. China and Russia want the UN General Assembly to adopt their International Code of Conduct for Information Security that would give governments more of a role to play, and greater control on content.

These countries would like the UN's International Telecommunication Union (ITU) to have a supervisory role, something firmly resisted by the U.S. and other Western countries. "The UN is a forum and not the right place to make decisions," says **Frank Asbeck**, Counsellor for Security and Space Policy at the European External Action Service, the EU's foreign diplomatic arm. "We are living in an environment where we need pragmatic and socially acceptable solutions quickly. We can't get into negotiations that take decades."

Many Western governments prefer a multi-stakeholder approach, like that promoted by the Organisation for Economic Cooperation and Development

(OECD). "We should keep the multi-stakeholder approach," says Asbeck, "while at the same time seeking optimum balance between enterprises, governments and law enforcement institutions. My guideline would be as much state involvement as absolutely necessary, but as little as possible."

Internet governance

Who gets to control domain name systems? Western governments would like to reign in some of the influence of the Internet Corporation for Assigned Names and Numbers (ICANN), the internet's address system, one of the few bodies with a global, centralised influence in the internet. Other countries would like to see the ITU in charge of domain names. The ITU also involves multi-stakeholderism, but under government leadership, which worries many internet community actors.

The U.S.-based, private-sector-led ICANN, which brings together net users, the private sector and government, manages IP addresses, assigns numbers, and handles domain name registration and its management.

"The issue between ICANN and the ITU is multi-stakeholderism," says **Stefano Trumpy** from Italy's National Council for Research. "This worries many people. At the IGF in Nairobi in September 2011, India, Brazil and South Africa suggested setting up an ad hoc committee within the UN to deal with public policy concerning the internet, including standards. It's a worrying idea. Standards were started by the private sector and shouldn't be controlled by government."

"There is no perfect governance model," says Trumpy. "It has to evolve and gain the confidence of the world community via continuous updates and a quest for transparency, and by listening to different stakeholders to arrive at decisions."

Standardisation

Technical standardisation is the second component in the governance of cyber-security and it is currently in the hands of the Internet Engineering Task Force (IETF), which collaborates with the ITU and industry. "We need an open process," says Japanese expert **Suguru Yamaguchi**, "with the open participation of industry and the public sector." Several other venues are competing to handle global inter-operability and common criteria, among them the International Organisation for Standardisation (ISO), and the professional association, the Institute of Electrical and Electronic Engineers (IEEE).

Law enforcement

The third component is law enforcement. Interpol has designed a strong legal framework, and other international frameworks are being set up.

Interpol's framework is used to handle cyber-crime from countries that don't have a legal framework on cyber-crime.

Many countries believe in the effectiveness of the 11-year-old Budapest Convention, the convention on cyber-crime that allows authorities in one country to pursue criminals in another. The U.S., Japan and Canada have signed up, but others haven't and don't agree about the meaning of cyber-crime. Russia, for instance, opposes the idea of "trans-border access", preferring a UN treaty that would respect borders.

Information-sharing

The fourth is information-sharing. Sharing information globally is a global headache but it's key to internet hygiene. The global Computer Emergency Response Team (CERT) forum called FIRST does this very effectively, but no one thinks that's enough. 'We need more and more collaboration to encourage global information-sharing," says Yamaguchi.

Among the bodies looking at the issue, the ITU-sponsored IMPACT in Malaysia is an advance warning system in the telecommunication community. "The issue is that it's all very well telling the U.S. there is a problem but what can the telecoms do about it? ," asks Accenture's **Alastair MacWillson**. The U.S.-based Meridian Conference and Process, with its annual CIIP conferences, is another key player in trust-building and international cooperation. Aimed at senior government policy-makers, it is open to all countries.

Concern about state-supported attacks often gets in the way of information sharing. In many regions, special fora have been set up, like the Asian Regional Forum (ARF) sponsored by the ASEAN+6 countries to ease tension in the Korean peninsula.

"Still there is a basic lack of trust among some countries and we need more open dialogue to ease that tension," says Yamaguchi. "Hope may come from industry. With many firms now going global, they are quite open and aggressive about sharing information with various entities. I hope that global companies can act as catalysts to encourage governments to open their door to dialogue."

THE ITU TAKES ON SMART PHONES

"It took 125 years for fixed phones to reach the first billion, and only 11 years for the mobile phone to do so," says **Hamadoun Touré**, Secretary General of the Geneva-based International Telecommunication Union (ITU). An engineer by training, he says fibre optic networks are speeding up our worldwide connectivity much faster

than he had expected. “With broadband, the volume of data is going much faster than infrastructure growth. That’s a little worrisome. We risk a traffic jam in cyber-space.”

The Broadband Commission was set up in 2010 to address the issue of fast growth. Touré stresses that a high-speed, high-capacity internet is essential to achieving the Millennium Development Goals. “Broadband improves healthcare, education, energy efficiency. It’s a global phenomenon and its safety needs a global response done in a global framework of cooperation.” Touré insists that security in cyber-space is the same as security in the conventional world.

A first and easier step at creating a global framework is the Child Online Protection Initiative (COP), aimed at protecting children in cyber-space. “Children are our most common denominator,” says Touré. “Whether or not a country legalises pornography, everyone agrees that child pornography is a crime. It’s easy to take concrete action in that direction. The same type of work can then be done in other areas.”

Touré says the next war will take place in cyber-space. With criminal activities and espionage on the increase, he firmly believes we need a global cooperation framework. His view is that an ITU cooperation framework would be negotiated “around a large round table. It wouldn’t just involve our 193 member states, but also the private sector and consumer groups. Are we ready for such a negotiation? We have no choice. We have to do it for the safety of our children, our businesses and our countries.”

Touré’s to-do list

- Increasing access to broadband as a way of helping people increase social and economic development.
- Increasing global efforts to coordinate cyber-security, and making sure governments work hand-in-glove with the private sector. Ordinary users also need to feel comfortable with their own security.
- Spectrum allocation: 2015 is the deadline for the move over from analogue to digital broadcasting. A serious technical discussion is about to take place about what to do with the freed-up spectrum.
- Preparing for the review of the international telecommunication regulations. The 1988 agreement is obsolete. Now that so many new systems and technologies have come into place, issues and priorities have changed completely.

Section V. Breaking down the walls between the cyber communities

To achieve workable international rules governing cyber-space, the walls dividing sectors, countries and even generations must be razed

Cyber-space is honeycombed with walls. There are walls between generations, walls between professional sectors, and walls between countries. The trouble is these walls aren't built on hard ground and they make little sense. In as global and porous an environment as cyber-space, the building of any legal and regulatory framework needs specialists to broaden their outlook and countries to work together.

"Governments tend to move slowly, but with cyber-security we need to move fast," says cyber-security advocate **Tim Scully**. "Cyber-security is a social problem, not just a military problem. We talk in terms of national security, but we should talk in the context of national interest." He talks of the need for strong collaboration and leadership trust between government, industry and academia, more so than in many other areas. Australia's Cyber White Paper to be published in 2012 is a step in this direction.

The generation divide

The most archaic divide is between generations. Many experts mention that their children's view on internet privacy is completely different from their own, epitomised by their attitudes to social networks.

"If an information security person is not using Twitter or Facebook, he is not in the right place to make a decision about the use of those tools"

William Beer

"My kids' generation has no fear of computers and they don't care about privacy," says British cyber-expert **Peter Sommer**. In 2011, when Sony's 77 million clients' personal details were hacked, the company shut its PlayStation network for two weeks. Most young users were angrier at not being able to play than about the privacy breach.

When citing this incident, Sommer says he makes no value judgment. He thinks the Sony incident was symptomatic. "You have to be very careful if you're right or wrong about this. I think the younger generation often see us as boring old farts and they may be right. It's a changing world."

Canadian specialist **Rafal Rohozinski**, CEO of the SecDev. Group, thinks the generation divide is a very real problem. "Policy-makers are often 10 to 15 years behind the internet generation, and they are dealing with questions they can't really understand." Not only that, adds **William Beer**, who heads Information and Cyber-security Practice at PwC, but these same policy-makers need to take into account that technology has permanently changed younger people's conception of privacy. He goes a step further. "If an information security person is not using Twitter or Facebook, he is not in the right place to make a decision about the use of those tools."

Improving trust between industry stakeholders

Private companies are fearful that information they provide could be misused by government or the competition. Experiments in trust-building are going on around the world, and this often means working with competitors. As a result of growing fraud, the U.S. financial services set up the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share information on attack techniques and cyber-threats to the banking systems. On a much smaller scale, the Belgian Financial Sector Federation (Febelfin), with 238 members, does similar work using freelance experts.

A comparable initiative has been set up by the oil and gas industries in the wake of the so-called Night Dragon attacks that brought down and reconfigured systems. It is FS-ISAC's global mirror. "For the first time, several big oil companies have got together," says Accenture's **Alastair MacWillson**, "to start a communication chain that has turned into an industry group. These are early days but I predict more and more of this happening at industry level around the world."

Overcoming the barriers between rivals

That information-sharing is to the advantage of professional competitors and should be obvious says researcher **Costin Raiu** of Kaspersky Lab in Russia. "There are benefits for everyone. Governments and the military will see marked improvements in their security. Academia will be able to develop new protocols and design new architectures. And if users are better protected, cyber-crime will go down."

William Beer, head of security at PwC, thinks that facilitators can help these professional groups communicate. "I work with behavioural guys," he says, "because they can help understand what makes a military professional tick, or what makes a businessman or woman tick, and how you take that into

account to share information. We have relied too long on security people with their slightly restricted skill set. Industry has used the techno language far too long."

Are cyber-crime and cyber-security one and the same?

Take crime busting. In this world of blurred boundaries, the distinction between cyber-crime and cyber-security may not be a useful one to make. A better focus, says **Victoria Baines**, strategic adviser on cyber-crime at the European law enforcement agency Europol, is to have a collaborative response to regional and global threats, and to encourage the private and public sectors and academia to work together.

She cites as an example the successful dismantling in 2009 of Spain's notorious Mariposa cyber-scam botnet, for which academics, the military, law enforcement, the private sector and third countries worked together to bring down. "What Europol and Interpol bring that was lacking before is international coordination of cyber-crime," she says. "More than for other crime sites, you can't investigate cyber-crime within national boundaries."

"We deal with automation of malicious software distribution, denial of service and the money-making side of things," she says, "but we are also very active in coordinating responses to cyber-crime when it comes to hackers employed in the forums of the underground digital economies. These people hack for dollars, they often don't know the real identity of their bosses and they're spread far and wide."

"More than for other crime sites, you can't investigate cyber-crime within national boundaries"

Victoria Baines

Steps towards global sharing

One step among others towards sharing information about the cyber-threat between countries in the East and West is being handled by Malaysia-based IMPACT, the education, training and information-sharing arm of the ITU (the United Nation's agency for information and communication technologies). Chairman **Mohd Noor Amin** is a firm proponent of the multi-stakeholder platform approach. "The final user has to be educated to behave responsibly," he says, "and the private sector and governments have to invest in security, despite the shortage of money." Some 137 nations have signed up as IMPACT partners, but Amin stresses that countries that haven't, like the UK and the U.S., engage actively. "They know you have to connect with the rest of the world. It's only a matter of time before every country joins."

Section VI. The private sector's privacy dilemma

Commercial secrecy is of key importance to companies investing in cyber, but it also risks compounding the problems of cyber-security and its dangers

In many people's view, the Netherlands offers the best example of successful private-public partnerships with its platform for cyber-security, a sort of cyber-exchange. "It's an excellent way of discussing the issues and translating them into some form of action, and even voluntary or mandatory regulations," says **Alastair MacWillson** of Accenture. "Much more of this should happen globally."

Good work is also being done in the United States. But around the world, the public-private partnership tends to be advancing very slowly. Some countries like France are suspicious of an overly close relationship between the public and private sectors.

Why the private sector would be better advised to share information

The private sector comes at cyber from a specific angle: the money-making angle. And as **John Meakin** who heads cyber-security at BP points out: "If you take the risk out of business you will never make a profit."

But the private sector also has valuable "real-life" experience of cyber-attacks. The problem is that companies are reluctant to talk about these; they aren't keen to reveal vulnerabilities to competition or to consumers, and they also have data privacy rules to contend with. "There's naturally a healthy dose of scepticism on both sides," says **William Beer**, director of cyber-security at PwC. "The views of the threats are not the same. "

One thing is clear; in order to have a good picture of the risks and dangers on the internet, the private sector has to share information with the public sector and vice versa. For instance, are a series of cyber-attacks directed at governments somehow related to similar attacks aimed at financial institutions?

The next step is to pass on this information the researchers and scientists. "We can't have security and obscurity," says researcher **Jesus Luna** of the Deeds Group. "Academia can provide the algorithms and the techniques, but we are missing the data that validates our research. We need that private and public information."

More exchange of information is going on than we think, says **Costin Raiu**, researcher at Kaspersky Lab in Moscow, but a lot takes place very discreetly. "It might look like companies are not sharing much information," he says, "but it is happening in closed discussions, for instance in computer and anti-virus research organisations. You have to remember that this can be a risky business. In countries like Brazil, we have seen death threats against security experts."

Making regulations that make sense for everyone

On the one hand, the academics and the security sales people are saying, trust us with your data and we'll provide you with better security mechanisms and assurance levels. At the same time, policy-makers are saying let's come up with rules and regulations to make this a safer playing field. Even if many argue that regulations are necessarily soon obsolete, cyber-security advocate **Tim Scully** points out that the enforced wearing of seatbelts in many countries may not have eliminated road deaths, but it has saved lives.

"Of course regulation has a part to play," says **Judy Baker**, a former civil servant who is now director of Cyber Security Challenge UK, "but it is rarely the whole solution. It takes time to implement and the problems it is designed to address are constantly changing. Regulation is always behind the curve." But one thing is sure: any discussion must engage the private sector, she says, if we are to ensure that regulation make sense. She adds that the cyber-threat is best dealt with in a "business as usual way" if things are not to enter an escalatory cycle.

Governments too often come up with a good idea but have a hard time implementing it because they lack experience of the service world, says **Vytautas Butrimas**, Chief Advisor for Cyber-Security at Lithuania's Ministry of Defence. "If the private sector is brought in early during the planning and drafting phases, then it is much more likely that the regulation will not have to be changed or adjusted right away. And at least the process will provide both sides with an understanding of each others' interests."

"The people who write regulations and standards are by nature not particularly well connected with business strategies and needs," says Accenture's **Alastair MacWillson**. "Governments should pull together business and get them involved in the drafting of regulations, and facilitate that dialogue in how they deal with this without stifling business, in the way the Dutch are doing it."

Most governments recognise that they could do a lot more to facilitate knowledge, and that this implies dealing with commercial sensitivities so as to know how an attack took place and what techniques were used to carry

it out. "We must remove penalties on an organisation that has been hacked and that has lost data," MacWillson says, "or there is no motivation to declare the attack. We need a no-blame sharing of information."

The blame game: From software companies to service providers, who should be responsible for what?

Certainly, pointing the finger of blame isn't the way to go. Some experts suggest that software companies should be made liable for attacks arguably due to their own poor coding. So far, software companies have no liability, as printed in small lettering in their contracts. "They should be subject to more pressure than they are today," says BP's security chief Meakin, "but I'm not saying they should be made liable."

One-hundred percent security is not achievable, and systems are vulnerable to cyber-attacks for a slew of reasons, including the lack of an appropriate security policy and misuse by users. "People readily point the fingers at villains in the software community," says MacWillson, "when they haven't done their updates. There are too many people in the whole chain to pinpoint a single villain."

Section VII. Bearing the costs of cyber insecurity

Cyber-security doesn't have to cost a lot, but should business or government shoulder the greatest part of these costs?

Kamlesh Bajaj, CEO of the Data Security Council of India (DSCI), thinks government should pay a proportion of private company investment. "Critical infrastructure is essential to the functioning of a country, and government should pay private companies a proportion of their cyber-security private investment. What if a bomb was dropped on a bank? The government would help. A logic bomb dropped through networks to decapitate the systems is not that different."

Frank Asbeck of the EU's new diplomatic arm, the European External Action Service, thinks a secure internet is a major support for getting out of the economic crisis. "There are areas of the economy where cyber-space and the internet play a huge role," he says, "and investing in cyber-security means making it and cyber-space reliable and trusted. In areas like banking, the communication business, the optimisation of energy usage and smart grids, you can use information technology to save resources and to operate much more efficiently."

If we look at econometric models for calculating the costs of individual cyber-attacks, we are getting there very slowly. One of the problems is the wide variety of people collecting the information and drawing up the statistics; the other is that companies tend to keep this sort of detail very close to the chest.

"We don't have actuarial tables," says Canadian **Rafal Rohozinski**, "but they will come. The U.S. has signed a non-binding agreement that companies report on breaches and loss of intellectual property. Over time, insurance will move from the realm of hype and speculation to businesses."

"The insurance industry too is getting there slowly, although in Europe we still mostly have insurance companies designed on the 19th-century British model, and the attitude tends to be, 'so long as it hasn't happened, we'll wait and see,'" says **Lars Nicander**, Director of the Centre for Asymmetric Threat Studies at the Swedish National Defence College.

"What if a bomb was dropped on a bank? The government would help. A logic bomb dropped through networks is not that different."

Kamlesh Bajaj

THE INSURANCE SECTOR WAKES UP

"A cyber hacker is nothing more than a bank robber using another weapon," says **Larry Collins**, left, head of e-solutions at Zurich Financial Services. "His motivation is robbery and theft."

The issue, he says, is that suddenly new systems sprang into existence with valuable information stored on them. With millions and millions of credit card numbers, the insurance sector got scared. "The whole computer world is changing rapidly," says Collins. "Premiums and costs are set actuarially based on what happened. When new things happen how much is that worth?"

Do we need to take out special insurance? Yes, says **Tim Stapleton**, pictured, Zurich's Professional Liability Product Manager. One problem is that insurance companies are increasingly denying coverage on non-traditional claims. Small and medium-size businesses in particular need to have dedicated insurance policies that cover expenses in case of cyber-attacks, he says, but that also give faster access to specialised resources so they can get the ball rolling and figure out what happened.

According to Stapleton, today's hottest cyber debates in the insurance industry are about privacy regulations, litigation trends and general privacy practices. "What kind of information is the company collecting, how is it storing that information, how is it using it once in its possession, how is it securing it? Most companies post privacy notices outlining these elements. Where we run into problems is when they haven't complied with those privacy notices."

Insurance companies have different ways of labelling cyber-liability. They don't even describe it the same way: some talk of "information security and privacy"; others say "cyber", still others say "network security". In the U.S., basic coverage includes core covers, like privacy and security liability coverage that provides defence and indemnity for third party claims, including class action by individuals or from banks if they have to reissue payment and credit cards; and first party (the insured person's) privacy breach costs that would apply before a claim at the time that the event occurs. There are also services provided by vendors contracted by the insurance company, such as credit monitoring, forensics, notification and public relations costs to offset damage done to a company's reputation.

What are the rules of insurance against cyber-attacks?
The triggers for a cyber-attack generally concern privacy, Zurich's experts say, like the disclosure of personal data – a name along with social security or

Great minds don't think alike

Kofi Annan, Anders Fogh Rasmussen, Carl Bildt, Javier Solana, Connie Hedegaard, Wolfgang Schäuble, Anna Diamantopoulou, Nicolas Sarkozy, Guy Verhofstadt, Pascal Lamy... Find out what the key decision-makers are saying in *Europe's World* - and join the online debate yourself at **europesworld.org**

Europe's World
The only Europe-wide policy journal

driver's licence numbers. This sort of disclosure can also happen because of a network problem or a careless event, like losing a laptop or leaving a file in a public place.

How do you balance risk and liability in case of attack?
Privacy breach costs are a loss leader at the moment, say Zurich's specialists, because the trigger is much more sensitive – it's the mere fact that an event occurs. That's why many carriers lower the limit on liability to control costs, although the increase in online breaches means that data is fast accumulating on the costs to companies.

How much has Zurich been paying out?
"We have been paying out at both ends – first party costs and third party liability," Stapleton says. "You can generally predict that if sectors like healthcare, a financial institution or a retailer get hit, they will have more personal identification on hand and it might cost more to respond to a breach in defence costs and settlements. A manufacturer may not have as high a volume of personal identification information and may cost less."

What proportion of an electronic info system's budget should be invested in cyber protection?
"Enough to protect the company against harm," says Collins. The size of the effort needed to protect a system has to be proportional to the sensitivity of the information held on site. "Our advice to companies is to do two things. Take a look at what you're storing and who has access even internally. Then we always advise using scenario-based risk assessment; looking at things from a business model point of view makes a great deal of sense."

Top threats

- **Cyber hacktivism.** The concern is that they could take down major sites, or block e-commerce money and damage databases.
- **Cloud hacking.** Problems posed by a central repository holding data and information for thousands of companies. The scare phrase is "hyper-jacking", or breaking into many systems at once. It's been done already: hackers have exploited vulnerabilities in cloud architecture.
- **Mobile and tablet hacking.** Hackers can breach our mobile device within 15 minutes at most.
- **Advanced persistent threat.** This is where the cloak-and-dagger comes in. Sophisticated, highly professional groups perhaps organised by intelligence agencies or well-funded criminal gangs.

Section VIII. Private citizens : issues of freedom and protection

Among the many complicated problems cyber-security raises is that of security versus privacy. Are they opposed? Or can they co-exist?

"It's an incredibly confused picture at the moment," says **Alastair MacWillson**, managing director of Accenture's global security group. "Views on security change with the age of users. The young are less concerned about privacy but they want full access. You also have higher or lower sensitivity to privacy issues in different countries."

China and Russia for instance consider that the cyber-threat also involves propaganda and threats of political unrest, and thus should allow content censorship. During the Arab Spring, the Egyptian government threatened to cut internet access, although they didn't in the end. In Europe, countries that have experienced communism tend to be more aware of privacy issues than others. So is Germany, with the added memory of Nazism. But within countries, there are arguably as many views or non-views as there are users.

"Can you have cyber-security without a Big Brother state?" asks **Fred Piper**, who runs Codes & Ciphers Ltd, a British consultancy that offers advice in information security. "The more governments impose, and the more secure they can make the system, the less freedom you've got." In the UK, he says, "the debate compares computers to cars and goes as follows; the motor industry has worldwide standards of behaviour; it is acknowledged that it takes a certain amount of skill to drive; therefore you should need a licence to use the internet."

"You have to define the field and not confuse democracy with security," says **Stefano Trumpy**, research associate at the Institute for Informatics and Telematics of the Italian National Research Council (CNR). "If you look at the social stability assured by local and international law enforcement agencies, there is a serious risk that freedom of expression will face undue limitations. Freedom of expression is a basic principle and using security to limit it is not a good thing. Law enforcement agencies should operate in a clear and transparent way so that internet users understand the frame of prevention/intervention in cases of cyber-crime."

"The trade-off doesn't make it worthwhile," argues **Sandro Gaycken**, a German philosopher of science and technology. "The first point is that the most effective attackers are not identifiable, so they can't be prosecuted. The second, is that in order to identify a perpetrator I have two options. I can look into every package on the web for malicious content or I can store the content and look at it after a few months. Both options involve looking into each and every data package. It's not efficient and there are too many trade-offs."

"Most people's knowledge is confined to the Matrix movies and the books of the Millennium Trilogy"

Judy Baker

Internet responsibility, from private users to corporate giants

Gaycken's view is that it is more efficient to secure the systems themselves by raising the average user's understanding. "Users should be more aware of the business models used by criminals. We need to raise overall security awareness." He says that concurrently we can do things against denial-of-service and other more sophisticated attacks, such as disconnecting the internet and using closed-system models. "It shouldn't be about the control of networks over the security of hosts," he says.

For **Olivier Caleff**, who works for the French consultancy Devoteam that gives advice on cyber-security, education and training are key to combating the cyber-threat. "I would say that's 80% of the solution," he says. "People are using computer mobile phones and too often they believe everything they read. They trust the most stupid messages."

Too many people will blithely hand out their details on the internet, or think they are addressing air-tight user groups when in fact they are part of a very open session. They aren't aware that their data is being sent on to other companies. Like many others, Caleff believes that education should start in school, and that companies, whatever their size, should be responsible for educating their employees.

The cyber-security skills gap

If we're talking education, we come to the fact that most countries are crying for people to do cyber-security jobs. "It's an immature profession," says **Judy Baker** who runs Cyber Security Challenge UK, an organisation that recruits

talent through national competitions and games. The same recruitment methods are used in the United States. When the Centre for Strategic and International Strategies (CSIS) advised President Barack Obama that he needed 10-15,000 more cyber-security professionals, they ran competitions to encourage people to identify talent. "You have a lot of well-hidden front doors," says Baker.

The SANS Institute in the U.S., a research and education organisation, found that 90% of companies can't get the cyber-security people they need. They list eight categories of jobs, from technical to strategic.

"We need to introduce cyber-security into school curricula," Baker says. "Most people's knowledge is confined to the Matrix movies and the books of the Millennium Trilogy. In the UK and in most countries, it's only when you get to post-graduate levels that it is taught seriously. It's not surprising that people are not considering it as a career. And we're looking for people with creative skills. We need people who can find ways to do things differently, rather than run behind the problems in a patch-and-pray position."

"People too often believe everything they read, and trust the most stupid messages"

Olivier Caleff

PART TWO

Section I. A worldwide brainstorming of experts

In this global survey conducted by the SDA in late 2011, some 250 respondents were asked to rate the countries – other than their own – they deemed best prepared against cyber attacks. The U.S., the UK and Estonia topped the list, while Albania, Mexico and Romania bombed.

What is the simplest way to improve international cooperation in cyber-space, the SDA asked 250 senior security practitioners in a global conversation last November. By improving information sharing, engaging in more cyber exercises, incentivising, creating common standards, drawing up a non-binding convention, giving more power to Interpol, launching public awareness campaigns, and by talk, talk and more talk, they replied. Many participants in this Call for Ideas mentioned legal frameworks, standards, protocols and codes of conduct, and increased cooperation between national CERTs.

This global conversation was particularly relevant because of the high level of participants from 35 countries that spanned Albania to the United States. They included staff at the EU, Interpol, Eurocontrol, the UN, NATO and the OSCE. We also heard from ministers of defence and the interior, MPs and MEPs, top-level ministerial staff, academics from universities from across the globe, as well as NGOs, think tanks, trade associations, and private companies including banks, IT specialists, defence groups, consultancies and law firms.

The prevailing view from Australia is that norms are essential, as is the need to "recognise the inherent national construct of cyber space". An Austrian expert, on the other hand, feels that the simplest way to improve cooperation in cyber space is to "exchange important information among stakeholders".

A Belgian expert believes that in the absence of a global regulatory body, the simplest solution is for "countries to regularly participate in joint exercises that foster international cooperation and the coordination of national policies." Another feels that the way to go is to use existing structures and organisations like NATO, the OSCE and the Council of Europe. Another, more jaded, Belgian respondent feels that "if it was that simple it would already be in place" and a third, somewhat catastrophist compatriot suggests a "cyber 9/11" will do it.

One public sector respondent from Denmark shaped his views clearly. "First of all, make it a topic of equal importance to all nations. The level of international cooperation can only be raised as high as the lowest common denominator. When that threshold has been reached, it's a matter of multinational and bilateral cooperation – within or outside existing organisations. The issue of cooperation is best approached from a business and commercial angle; a security or values-based approach would only lead to an escalation of conflicts."

Northern Europeans, generally considered to be among the world's cyber-security leaders, tend to argue that there is no such thing as an easy answer. "More awareness, and better sharing of information and best practices, are a good starting point," one Estonian says. "International projects and seminars to foster common understanding, says another. "Sit down at the same table and initiate a discussion," concludes a Finn.

"It's time to locate thinking about cyber-conflict into the framework of existing international law and strategy"

James Lewis

In Greece, one expert's view is that "cooperation is always complex, and cyber-space is no exception." Getting in the way are "political games, the different interests of nations, corporations, organisations, institutions and even personalities". A radical stance from India suggests "Ostracise countries that don't adhere to internationally agreed norms on cyber security, and kick them off the internet."

A three-step approach suggested by an Icelandic expert: Start by establishing which practices – ie criminal phishing - are universally disapproved of by states, and erect defences against them. Then consider which existing international agreements and standards against economic and civil crime apply. And thirdly, use the Council of Europe's cyber crime-convention as a legal basis.

From the U.S., the main message is to go for norms and rules, but also build trust between parties by joining organisations like FIRST, and by creating an international body of "key empowered stakeholders representing each country's interests. "Do not use the UN model, which is entirely ineffective." "More dialogue at the UN", another says firmly.

Key attitudes

- Damage or disruption to critical infrastructure is seen as the greatest single threat posed by cyber-attacks, with 43% identifying this as a national threat with wide economic consequences. Some 15% consider cyber-espionage, along with theft of personal data and intellectual property, as the greatest threat. A further 10% believe that cyber-attacks damage the credibility of governments and organisations and our trust in them.

- The term cyber-war is considered inaccurate or outright scaremongering by 26% of respondents, while 45% believed it is accurate.

- Missile-defence is as important as cyber-defence according to 38% percent of respondents. Almost the same number (36%) believe cyber-security is more important.

- In contrast, views are divided between those who think that cyber-security is as important as border security (45%), and those who see it as less important (35%).

- 63% of respondents agree that cyber-security must be protected from budget cuts while only 8% believe it shouldn't.

- Roughly the same proportion (62%) consider that cyber-space is a global common like the sea or space.

- Over half (57%) believe that an arms race is taking place in cyber-space, while a large majority (84%) see cyber-attacks as a threat to national and international security, and to trade.

- Although almost everyone believes that cyber-security exercises are important, only a fifth of those surveyed in the private sector have taken part in such exercises (21 % in international exercises and 22% in national exercises).

- Over two thirds (67%) see the need for more government regulations in the private sector.

- In both private and public sectors, more than half (56%) highlight a coming skills shortage.

Section II. Country-by-country stress tests

There is a cyber-security paradox: the less sophisticated and widespread a country's connection to the internet, the lesser the cyber-threat. The more services are on line, the higher the risk of cyber-attack. On the other hand, the countries best prepared to react to a cyber-attack are those that are cyber and internet literate.

"The U.S., the UK, Israel and the Nordic countries are all IT literate," says **Lars Nicander**, Director of Cyber-Security at the Swedish National Defence College. "But if you can defend yourself, you also can attack – Israel, China and Russia are the most consistently offensive countries."

John Meakin, BP's director of digital security, holds the view that although China is among the countries to play a more aggressive role in cyber-space, mainly related to espionage, "it has such a controlled social, political and economic system that what we label as government, say in the UK or the U.S., is not at all the same in China. The spread of activities is much broader."

As a result, Meakin believes the West should engage China and Russia in a multi-national governmental dialogue. "It isn't the case that in China a single government department is doing all the bad stuff. By incentivising these countries to gradually change, we may gradually reduce the number of attacks."

In the words of **Stewart Baker**, partner in the U.S. law firm Steptoe & Johnson who was formerly with the Department of Homeland Security, different attitudes to the governance of cyber-space in the West and countries like China and Russia are likely to create problems.

"We in the West are going to face a tough choice because the governments that don't like free speech on the internet are going to put us in the position of choosing between free speech and cyber-security," he says. "There is a conflict there. You can't have a lot of anonymity on the internet and still have cyber-security. As soon as you start protecting anonymity, you are going to face hard decisions. I don't think we're served well by the foreign ministries that say we can have it all."

Most countries have set up national CERTs or teams of IT security specialists who can respond in case of crisis, and most are engaging or attempting

to engage in constructive dialogue with the private sector which owns the national critical infrastructure. More and more countries are taking part in global exercises that allow them to test scenarios and know who to contact in an emergency.

"The governments that don't like free speech on the internet are going to put us in the position of choosing between free speech and cyber-security"

Stewart Baker

What do CERTs actually do?

"A whole range of preventive measures," explains **Freddy Dezeure**, head of the European Commission's inter-institutional emergency response pre-configuration team. "They'll see what's happening on the internet, they'll inform their clients and maybe protect their systems, and make sure their constituency is informed." To be a member of the increasingly important international CERT community means complying with such basic requirements as accessibility functions and operating procedures.

Most countries around the world are developing or updating national cyber-security strategies to defend themselves against the variegated forms of cyber-attack, with some 40 or so cyber-security strategies articulated or published around the world.

William Beer, Director of Information and Cyber-security Practice at PwC, has read a number of these cyber-strategies, and he has a warning. "They tend to contradict the concept of cyber," he says, "which to my mind is about a global approach to interacting and transacting. It's about looking outwards. National cyber-security strategies have to be set in a global context, and they tend not to be."

Almost everyone agrees that with the U.S., the Nordic countries score high on cyber-security. "There is a general perception that the further north you go in Europe the safer your environment becomes," says Danish expert **Christian Wernberg-Tougaard**. "The Nordics have a tradition of information-sharing and transparency. Many public and private sector systems are based on trust."

"Some countries are very good in one domain and others in other domains," says **Evangelos Ouzounis**, an expert at ENISA, the European agency in charge of expertise and information security. He says it would be very hard to agree on a benchmarking system. "You can do it at the scientific, technical and procedural levels, but if you start a discussion with the players it becomes a nightmare because nobody wants to score underneath the benchmark."

In the even-handed view of Ouzounis, "Scandinavia and Finland have a higher level of trust than other European countries, but their critical information infrastructure is more centralised. Germany is better at protecting its critical information infrastructure, but they're weaker on regulatory issues because so many players are involved. France has solved a similar problem by creating the national cyber-security agency ANSSI."

The Netherlands scores high on engaging the private sector and is often looked at as a model. "Our national laws are all very different," says U.S. consultant **Melissa Hathaway** who formerly advised the Department of Homeland Security, "and these laws can get in the way of an open exchange. The Dutch have got it right. The Netherlands has recognised that industry has to help solve cyber-security problems and they set up a middle party for information exchange. The UK respects confidentiality, and Australia has codes of conduct. Other countries are taking a more regulatory approach, like the U.S. and India, and France and China have super-empowered their government to deal with protection."

The economic crisis isn't helping with investment, with many governments reluctant to engage new budgets and with research funds generally shrinking. Training isn't meeting the demand. "There's a big gap between what the market needs and what universities produce," Ouzonis says. "Most universities don't produce cyber-security professionals but computer scientists with little specialisation in security. We need a pan-European curriculum for cyber-security."

But despite rising awareness in many countries, too many have not yet understood the cyber-security threat. "For various reasons, they don't have a sound approach or enough operation capabilities," says Evangelos Ouzonis. "Different political cultures complicate the scene."

The methodology used for rating various countries' state of cyber-readiness is that developed by **Robert Lentz**, President of Cyber Security Strategies and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. His Cyber Security Maturity Model is a five-step roadmap for reaching resilience, the ultimate goal for governments and businesses that want to effectively operate throughout a sophisticated cyber-attack.

The first step to reaching this ideal is to have people applying the basic rules of hygiene; the next is about using computer network defence (CND) tools like anti-virus, firewalls, intrusion detection/protection, and strong identity management (such as electronic signatures); after that come standards and data exchanges to create a robust and interoperable cyber ecosystem. When that level has been reached the move is to a more agile defence posture,

Australia

Government CERT (CERT Australia, since 2010), cyber-security strategy since November 2009

Score: ★★★½☆

Until late 2011, Australia's Attorney General was in charge of cyber-security policy and of streamlining work between government departments and setting up information groups to discuss problems like critical infrastructure protection. However, since December the responsibility is in the hands of Prime Minister Julia Gillard in a move to consolidate whole-of-government responsibilities, according to a spokerperson for her department.

Interviewed before the reshuffle, **Ed Dawson** of Queensland University of Technology said cyber-security policy involved most big companies, but that on the downside the private sector is loath to take responsibility and spend money. A Cyber White Paper, issued in late 2011, focused on how to bring together the various stakeholders.

"With electricity for instance," Dawson continued, "we'll have the distributor saying that cyber-security is the responsibility of the power generators. It's like they're waiting for an accident to happen." The government has proposed to partly fund projects in the area of critical infrastructure.

Australia's funding policy on the whole gets good marks. Queensland University of Technology is currently engaged in two large projects. The first, co-funded by India (to the tune of A$4.4 million), is researching denial-of-service attacks. "We're trying to see what sort of attacks are feasible, and we're developing mechanisms like cryptography to protect against them," says Dawson. The other is a five-year project on airport security worth A$5 million.

with innovative cyber-defences tapping into advanced sensors and intrusion prevention systems from the host to the gateways.

"It's like the water-tight doors of a ship," says Lentz. "They won't stop the torpedo entering the hull but they will contain the breach and highlight those breaches in the command centre with advanced forensics to allow decision-makers time to assess the damage with minimal operational degradation."

Ultimately, achieving a resilient cyber-maturity level means predictive cyber-readiness and agility in one's own area and with partners. This involves Supply Chain Risk Management, and comprehensive education and training, starting with the ordinary user to the core group of cyber-defenders. Lentz's criteria have been used for the scores below.

The Australian Department of Defence's Cyber-Security Operations Centre (CSOC) provides threat detection and mitigation for government departments and agencies, and the Department is recruiting an extra 130 cyber-security experts to work there.

The country is also promoting a voluntary code of conduct for ISPs to educate customers, offer better online protection, and quarantine infected users. "The problem with voluntary codes is their uneven application," says **Tim Scully**, CEO of stratsec and Head of Cyber-Security at BAE Systems Australia. The Australian Communications and Media Authority has a list of blacklisted sites, and requires Australian ISPs to filter them.

Communications Minister Stephen Conroy says that the blacklist targets only illegal sites, but some feel that the scope of the censored content is too broad. "Selling cyber security regulations is a brave thing for a government to do," says Scully, citing the public outcry at the government's attempts to introduce internet censorship to protect children from porn. In a country where most people are hostile to the idea of carrying ID papers, privacy is high on the agenda.

Austria

Austria has a national CERT (CERT.at) but no single cyber-security strategy. Three cyber-security strategy processes are currently being drafted by the federal chancellery, Interior Ministry and Ministry of Defence. The country takes part in all CERT communities, including inter-governmental ones.

Score:

Austria can boast one of the most sophisticated e-governments in the EU, with the use of digital signatures now widespread across most services. Yet despite its highly developed service economy, Austria is still working on its own cyber-security strategy, lagging behind most other EU countries.

Austria may also have been lulled into a false sense of security by its low rate of malware infection – well below the world average. This is explained in part by the country's size compared to Germany, but also by the close working rapport between ISP technicians and CERT.at and the speed at which internet security policies can be implemented, in part thanks to broadband.

A number of ministries claim responsibility for cyber-security, although the federal chancellery is its main coordinator. However, legal responsibilities aren't always clear and this matter is exacerbated by lack of political interest. "We also lack senior level leadership," says **Alexander Klimburg** at the Austrian Institute of International Affairs, an independent research centre. "Decisions are made, at sub-ministerial level. But without top leadership, things won't move."

Incidents and threats are handled by CERT.at, but companies are under no legal obligation to report security breaches. In general, Austria's approach to public-private partnership tends to rely on methods and tools dating back to Cold War days, although a programme for protecting critical infrastructure (the APCIP) should soon bring this up to date.

Austria is rapidly building up bilateral relationships with countries and international organisations, with emphasis placed on developing regional partnerships like DACH (Austria, Germany, Switzerland). The country is also strengthening its army's cyber defence structure; media reports say that cyber-defence is about to get substantial additional funding – with supposedly over 1,600 soldiers assigned to cyber-security. Analysts predict, though, that insufficient leadership makes reaching these figures improbable.

Brazil

Brazil has a cyber-security strategy, and a national CERT (CERT.br) that participates in the informal CERT communities. An Information Security Department was set up in 2006, and a cyber-security command in 2010.

"Brazil has been without a war for generations," says **Raphael Mandarino**, Director of Brazil's Department of Information Security and Communications (DSIC). "We don't see cyber-space as a battlefield. Our cyber-security system was essentially created to protect internal department infrastructure, which makes our situation quite different from that of the U.S."

So far, widespread police corruption and lack of legislation to combat cyber-crime have constituted the country's Achilles heel. A computer crime bill has been pending in Congress since 2005. In a country where internet banking is widespread (some 73m people on the internet, with more than half using online banking), bank Trojans reign supreme. Cyber-attacks on users are above the world average.

Infrastructure and technology across Latin America and the Caribbean (LAC) tend to be outdated, and that's still the case in Brazil. Policymakers know that if the region's largest economy is to be considered a safe place to do business, the critical national infrastructure, which is mostly in the private sector, must be better protected. With the 2014 World Cup and the 2016 Olympics looming on the horizon, the pressure is on.

The DSIC is in charge of security in all government departments. "Our main task," says Mandarino, "is to capitalise on people by training all government agents. We have 1.5 million servers in the country, and 2,000 people working on cyber-security in government." His mandate covers the public sector only.

"Brazil has been a party since its inception in the UN convention which is based on a more comprehensive, inclusive discussion"

Raphael Mandarino

Despite regular meetings with the private companies in charge of energy, communications, transport, banking and water, actual progress is slow, Mandarino says. "We also need to restructure our defence command," he says, "and we are working hard on producing a command, control software."

The government recently launched the Brasilia-based Centre of Cyber Defence (CDCiber) to protect Brazil from attack. "The big challenge for CDCiber may be the need to protect private infrastructure," according to **William Beer** who is in charge of cyber-security at PwC in London.

With the Organisation of American States (OAS), Brazil is contributing to a cyber-security culture in South America that also involves technical cooperation. Brazil has proposed a legal framework on cyber-crime to replace the Budapest Convention, judged too Euro-centric. "We believe countries should join a more global convention," says Mandarino. "Brazil has been a party since its inception in the UN convention which is based on a more comprehensive, inclusive discussion."

Canada

Canada has a national CERT, a cyber-strategy and participates in informal CERT communities.

Score: ★★★½☆

Canada's Minister of Public Safety Vic Toews launched a Cyber-Security Awareness Month in October 2011, but despite its ambitious national cyber-security strategy, the Canadian government's critics tax it with moving too slowly and not providing enough funding.

"Canada has interesting expertise but those capabilities are not reflected in government," says thought leader **Rafal Rohozinski**, who runs the Canadian SecDev Group. He says the Ottawa government "eviscerated" the country's cyber-security programme for budgetary reasons.

In February 2011, government departments and the Canadian Parliament's network were penetrated and sensitive data stolen. "There's a tendency here to be suddenly aware of the cyber-bogeyman rather than look at the problem in its totality," says Rohozinski. He points at Canada's funding of

NGOs as an area where the government has shown efficiency but says there's a long way to go on the cyber-security front.

Among the challenges Canada faces is the fact that Google has sited one third of its cloud computing in Canada, which raises issues of copyright laws and territorial security. "Is the information subject to U.S. law or Canadian law?" asks Rohozinski. "Who determines the final resting place of jurisdiction? These are interesting questions."

The government has put "lawful access" legislation before Parliament that would vastly increase the right of law enforcement to collect intelligence online, including forcing internet providers to hand over names, email addresses and telephone numbers of subscribers. The public debate between "security" and "privacy" is still raging.

China

China has a national CERT, participates in informal CERT communities, and has a cyber-security strategy.

Score: ★★★☆☆

It's hard to sort Western prejudices from what China sees as its legitimate political concerns. One radical and uncontested difference is that China sees information as a weapon and a threat to regime stability, a different cultural perspective that leads to different protection measures. The basic fact is that half a billion people use the internet in China, and that a third of the country is online.

"The Chinese talk about information-security, we talk about cyber-security," says **Herbert S. Lin**, Chief Scientist at the Computer Science and Telecommunications Board at the National Academy of Sciences, Washington, D.C. "They consider some information to be as big a threat to the country as an attack on its critical infrastructure. Anything related to information security that gets done in the name of political stability is a positive thing."

"The Chinese talk about information-security, we talk about cyber-security"

Herbert Lin

Says Lin, "The Chinese point out that we too in the West are concerned about internet content. Child pornography is content and we pass laws against it. If the West believes in some kinds of content regulation, they say, where do

you draw the line? The Chinese say, you have a view on what should and should not go on the internet, and why should your view prevail over ours?"

"One of the Chinese government's leading concerns is to work out how to obtain the economic benefits of an open internet, without sacrificing political control," says Lin. The government-operated Golden Shield, known in the West as the Great Firewall of China, blocks some content from entering or leaving China. The government also has a close relationship with Internet Service Providers (ISPs).

"In China's political culture, we see a person's privacy as subordinate to maintaining social order," says **Peiran Wang**, a visiting scholar at Brussels' Free University (VUB). According to Wang, China's most urgent cyber-security challenges include "establishing a coherent legal and regulatory system, and enhancing cooperation between departments. At present, the Ministry of Public Security, the Ministry of Industry, the Ministry of State Security and even the military are involved, and they don't communicate well."

According to Russia's Kaspersky Lab, the .cn top-level domain was hosting almost 20% less malware in 2010 than in 2009. This is thought to be the result of a new Chinese policy restricting the .cn domain name to registered businesses. According to the *People's Daily*, the government is toughening laws on the way hacking crimes are handled by courts. The security industry, however, is still in its fledgling years.

China's information warfare and cyber capabilities are little known, although it has military training centres that include cyber-war training programmes. There are reports that the Chinese military takes direct orders from the president but does not report to the civilian government, the Central Committee. There are other reports of a cyber militia, a "loose web of cowboy hackers" not formally connected to the military or to the government, who hack for vaguely patriotic reasons.

But whereas the U.S. has formally stated that it will abide by the laws of war if it is to engage in a cyber conflict, the Chinese have not made it clear if they share that view. "I've been told by people who talk to the Chinese at the senior diplomatic level that the Chinese believe there are currently no international laws that apply to cyber-war, although this position has not yet been stated in writing," says Lin.

China belongs to the Shanghai Cooperation Organisation (SCO), a grouping that links it with Russia and most Central Asian countries, and which has issued a code of conduct stating the principles they believe should govern the use of the internet, including the primacy of states. "Among other things, China does not want U.S. views to shape the use of the internet," says Lin. "They believe the governments of nation states should be responsible for specifying how those under their jurisdiction are or are not able to use it."

Denmark

Denmark has a national CERT, participates in informal CERT communities, is part of the National CERTs in the EGC group, and has a contingency plan for cyber-incidents. It does not yet have a cyber-security strategy.

Score: ★★★★☆

Denmark's Defence Intelligence Service is planning a cyber-warfare unit to protect the armed forces' technology from cyber-attack. Although the country's security strategy is principally defensive, the army has a "3rd Electronic Warfare Company" whose aim is to disrupt or exploit enemy communications. Meanwhile, internet service providers are legally obliged to report all cyber-security incidents.

"What will our role in the international community look like in the future? What are our commitments and engagements?" asks ICT specialist **Christian Wernberg-Tougaard**. "Among topics under discussion, should we share our air force with neighbouring countries more than we do so far? Could we rent capability from Sweden, for example?"

Wernberg-Tougaard is chairman of the Danish Council for Greater IT-Security that was set up four years ago. Before, internet security issues were spread out between different ministries and stakeholders. Now the independent group of researchers, and public and private sector companies tries to bring a holistic approach to the change from an analogue to a digital service society. "We've had a big impact on the mindset of the country's policy agenda," claims Wernberg-Tougaard.

"One of the good things about Danish society," he explains, "is that we digitised very early on, in the early 1960s. Every child is assigned an ID number (CPR number) minutes after birth. Within two hours you can find this number in more than 30 systems, automating interaction with the home nurse, the paediatrician and child benefit." The system has its weaknesses, as the risk of privacy intrusion is increased by the relative age of the systems and increasing theft of CPR-numbers.

A working-group on "IT-security Beyond Borders", under the auspices of the Danish Board of Technology (DBT), has developed recommendations to improve IT-security, and make the country a world model. So far, groundbreaking work has been done in the area of child protection; ISP providers have formed an alliance to battle child pornography and jointly close down sites and enable police to carry out investigations, using a joint codex.

Every year, the Minister for Science, Technology and Innovation (since the change in government in 2011, this is now split between several ministries)

submits an IT and Telecommunications Policy Report to Parliament. But on the whole, law enforcement is under-funded and under-resourced and concentrates more on old-style police investigations than cyber-crime. Denmark is to take part in the "Nordic Resource Network" which seeks to improve cyber-defences.

Estonia

Estonia has a national CERT since 2006 (CERT-ee) and a cyber-security strategy (since 2008). The country participates in informal CERT communities, and in the EGC Group of national CERTs. Estonia takes part in cyber-incident exercises.

Score: ★★★★☆

The massive denial-of-service attacks against Estonia in 2007 alerted the world to what a cyber-attack might look like, although the consequences were not nearly as bad as the international press suggested. "The banks quickly handled the situation," says **Jüri Vain** of Tallinn University. "The 90-minute block-out was fatal to no one."

Many countries are now looking to Estonia for cyber-security leadership, even if Canadian expert **Rafal Rohozinski** stresses that "Estonia is really too small a country to be a case study."

But it is clearly easier to get organised in a small country, and **Heli Tiirmaa-Klaar**, a senior advisor on cyber-security at Estonia's Ministry of Defence, says they coped very efficiently when put to the test. "We limited the damage by limiting connectivity to the outside world," she says.

The public sector quickly analysed and patched up the holes, and banks have since further increased security, electronic signatures, backup systems and firewalls. The defence of critical infrastructure is now very much top of the agenda, and with 75% of it in private hands, much emphasis is being put on private-public partnerships.

"We'd been building resilience long before the attacks took place," says Tiirmaa-Klaar. "Our new crisis management system is pushing for a public-private dialogue based on a voluntary approach. We are keen both to protect our way of life and to protect our business interests."

Tiirmaa-Klaar, who led negotiations with private sector leaders in 2008, stresses that not only is coercion unnecessary, but that general awareness in Estonia is much higher than in other countries. "Even retired people have long been using computers," she says. "We have such a low population density that everyone needs internet access."

The country has very secure national authentification services, which require two electronic signatures (the only other country to do this is Israel). It plans to update its cyber-security strategy in 2013.

"This will involve substantial reworking," says **Jaan Priisalu**, who heads Estonia's Information Systems Authority. He is also behind the Cyber Defence League, set up in 2009, a voluntary body of civilians who engage in defence exercises.

Estonia remains a fast-developing information society, and the first country in the world to have used e-voting in Parliamentary elections (in 2005). Since 2011, cyber-security is in the hands of the Ministry of Economic Affairs and Communication (MeAC) and its two main agencies: the Department of State Information Systems (RISO) and the Estonian Informatics Centre (RIA). NATO's Cooperative Cyber Defence Centre of Excellence is also based in Tallinn.

As elsewhere, funding and resources are in short supply. "If you live in Japan," says Tiirmaa-Klaar, "you invest in safety measures against earthquakes. We have to do the same. Europe is a seismic region in cyber terms." Not surprisingly, Estonia has also been a frontrunner in promoting international cooperation, and has cyber-defence cooperation agreements with the Baltic and Nordic states.

"If you live in Japan, you invest in safety measures against earthquakes, and Europe is a seismic region in cyber terms"

Heli Tiirmaa-Klaar

THE EUROPEAN UNION

The 27-nation European Union has no single approach to cyber-security, as this is currently handled by member states. Responsibilities are national, but EU institutions and bodies like the European Commission, the European Parliament, the European Council, the European Central Bank, the European Court of Justice and 55 others are working on setting up their own inter-institutional CERT, rather like a national government CERT. At present, this CERT is represented by a pre-configuration team.

Freddy Dezeure is the head of this inter-institutional computer emergency response pre-configuration team (CERT-EU). "We're not aiming to protect all citizens in Europe or to coordinate the other CERTs," he says. "Our scope is limited to the EU institutions, bodies and agencies. We want to become the glue, the catalyst to initiate new systems and foster information exchange."

Although they started only recently, Dezeure says this inter-institutional CERT is ambitious. 'Some EU member states already have very advanced and sophisticated CERTs," he says, "and we have to aim to be among the best governmental CERTs. It would be very arrogant of us to go to the UK, for instance, and suggest they do things differently."

"Technology develops very quickly and we have trouble following up with policy," says **Evangelos Ouzounis**, Senior Expert at the Crete-based European Network and Information Security Agency (ENISA), the EU's centre of expertise. "Over the last two or three years," he says, "there have been tremendous developments at member state level, and pan-European level policy is also catching up. We're working towards a technology-neutral strategy, something where the technology can change but not the policy."

The EU has 140 national CERTs, with some countries, like the UK, having both a national and a governmental CERT. The operational CERTs with international visibility can join the informal European Government CERT peer group known as ECG that is developing cooperation on incident responses between member states. Ten member states belong to the group, and ENISA is helping the others get up to scratch "through trust development," says **Andrea Servida** of the European Commission's Information Society and Media Directorate General.

ENISA, which has an inventory of private sector, academic and governmental CERTs across Europe, is helping to spread good practices and to establish standard baseline series, like a guidebook. In November 2011, the European Union held its first joint cyber exercise with the U.S., which ENISA facilitated.

In 2010, ENISA helped member states carry out the first pan-European cyber-security exercise. In 2011, the EU ruled that member states have to report incidents to ENISA on a yearly basis. "This is important," says Ouzounis. "2012 may see the first reports. We want to work together to develop a common approach that will create more insight into what's going on."

But as ENISA's technical department head **Steve Purser** stresses, "much work at ENISA is spent on educating citizens to the fact that cyber-security is crucial to tomorrow's security. When you walk down the street, you won't answer personal questions from a stranger. In the electronic world, people don't exert the same kind of prudence. Security requires people to behave the same way in the electronic world as they do in the real world."

"Technology develops very quickly and we have trouble following up with policy"

Evangelos Ouzounis

For **Gerrard Quille**, Specialist in Foreign Security and Defence Policy at the European Parliament, the Parliament's top priorities include how information technologies and human rights can work fruitfully together, and how cyber-security and internet freedom fit into the EU's foreign policy debate.

Things are also moving on the cyber-crime fighting front, with next year likely to see the opening of a European cyber-crime centre, and the coordination of on line internet crime reporting in EU members states.

Victoria Baines, strategic advisor on cyber-crime at the EU's law enforcement agency Europol, stresses that a feasibility study is under way and that Europol hopes its conclusions will be to host the cyber-crime centre in The Hague, building on Europol's IT infrastructure in the city. Last year, Interpol set up two strategic partnerships – it joined the Virtual Global Taskforce (VGT) of agencies dealing with child abuse on line, and it is now the strategic law enforcement partner in the International Cyber-Security Alliance (ICSPA), co-founded by McAfee, Visa and others.

Finland

Finland has a national CERT (CERT-Fi), participates in informal CERT communities and is an active member of the European government CERTs Group (ECG). The country also engages in regular cyber-incident exercises in the public and private spheres.

Score: ★★★★½

In 2011, the Finnish government announced plans to invest heavily in developing an arsenal of cyber-defence weapons, such as worms, malware and viruses, to protect military, government and private enterprise networks, as well as the country's critical infrastructure.

"The idea of a defence strategy based on attack as well as defence is still taboo," says **Timo Härkönen**, director of government security in the Finnish Prime Minister's Office. "The public debate on the 'counter-punch' has only just started."

The 2007 attacks on Estonia were closely monitored. Some sites in Finland were also affected. Finland, like the other Nordic countries, is highly connected and has been since the 1990s. By 2015, Finland aims to be the world leader in information security.

One of the liveliest debates is about the preliminary report for the country's cyber-strategy due to be ready by the end of 2012. "Right now, too many

authorities are in charge of too many systems," says Härkönen. "We need a common system or a limited number of systems so as to avoid fragile areas."

Härkönen's view is that the open government network doesn't present a great security risk. "Much of the information there is aimed at the general public. We simply have to accept that it will be attacked and invest in protecting more sensitive networks like those of the police, border guards and defence forces, and the government's own confidential network." In 2013, Finland will have a common secure network for all these authorities.

The Finnish mobile telecom operators have adopted a code of conduct ensuring basic protective measures for mobile phone content. Finland has a long and solid tradition of public-private partnerships, supported by the National Emergency Supply Agency. As for international cooperation, Finland fares well with active links to Nordic and Baltic countries. The effective national CERT has an automated service that collects and reports information security incidents.

France

France has a national CERT (CERTA), and participates in the informal CERT community and in the EGC inter-governmental group of CERTs. France has had a cyber-strategy since 2011 and takes part in cyber-incident exercises.

Score: ★★★★☆

"We're living in times that recall the 19th-century scientist Louis Pasteur," says **Patrick Pailloux**, Director General of the French Network and Information Security Agency (ANSSI), the national cyber-security authority under the Prime Minister. "That's when doctors started washing their hands and sterilising equipment, realising that they could no longer do things any which way. The same now applies to internet security."

"We're living in times that recall the 19th-century scientist Louis Pasteur, when doctors started washing their hands and sterilising equipment. The same now applies to internet security."

Patrick Pailloux

ANSSI has been up and running since 2009 to protect France's public systems cyber network. "Our first task is to develop cyber-defence operational

capacities, including rapid intervention after attack," says Pailloux. "The second is to improve the protection of our national critical infrastructure."

Pailloux says that not enough engineers and IT specialists practice the most basic "rules of hygiene" when using the internet, and that too few company directors even know what these are. "It's a big, big problem," he says. "Not just in France but worldwide." He believes the massive attacks in March 2011 on the ministries of Budget and Finance acted as a wakeup call to private companies.

Olivier Caleff, an analyst at the Devoteam consultancy, agrees about the lack of specialised staff working on cyber-security in government agencies and the police, but on the plus side, he argues that France has excellent security methodologies. "We have access to a lot of products from many countries. Our problem is that although larger companies are growing increasingly aware of cyber-security, smaller companies are not doing enough."

Some problems are linked to jurisdiction. "Over the last three years France and Belgium have seen a big increase in unsophisticated phishing attacks from North Africa against banks," says **Jean-Michel Doan**, cyber-crime analyst at Lexsi Innovative Security. "We try to put all the banks together around a table to make a joint complaint, but the problem in a case like this is law enforcement in North Africa."

Pailloux believes the best way to overcome private companies' resistance to security problems is to create an interface between the government and private companies. "We need such a body to look at whether there should, for instance, be a legal obligation to report incidents. So far in France, the telecoms have to report incidents, but so should the 12 sectors of critical infrastructure."

"France has a highly centralised system," Pailloux explains, "with a single agency in charge of cyber-security, which is both an advantage and a disadvantage. On the one hand we have good inter-ministerial connections; on the other there's too few of us." Some 200 people work for ANSSI at present, with 360 promised by the end of 2013. France's ambition is to be among the global powers in cyber-defence, and is so far engaged in bilateral relations with Germany, the U.S. and the UK.

France has controversial policies on internet censorship. Its Loi Hadopi of 2009 allows internet service providers to monitor French users for copyrighted music and videos. Users who don't respond to the ISPs' warnings can be taken to court.

Germany

Germany has a national CERT (CERT-bund), and a cyber-security strategy since 2011. It is also a member of the EGC group of government CERTs and participates in cyber-incident exercises.

Score: ★★★★☆

Germany's solid engineering and safety culture has given it a headstart in cyber-security. "But our problems are the same as everyone else's," says **Sandro Gaycken**, a professor at the Berlin Free University. "There aren't enough people teaching security, and there's not enough focus on inter-disciplinarity."

Unlike most other countries, Germany hasn't been hit really hard by the economic recession. Nevertheless, private companies are loath to invest in cyber-security and recently little additional government funding has gone into cyber-defence, despite the unsettling fact that Germany topped Europe's cyber-crime list in 2011.

"Companies still don't know what the loss of intellectual property means," Gaycken says. "The attitude is 'What do I care if China steals my intellectual property?'" On the other hand, according to ENISA expert **Evangelos Ouzounis**, Germany was an early starter in 2005 at protecting its critical information infrastructure, even if the regulatory system is complicated by the number of agencies at federal level – the three main players are the telecoms regulator, the Ministry of the Economy and the Interior Ministry.

Another early start for Germany is its central cyber-protection organisation, the Bundesamt für Sicherheit in der Informationstechnik (BSI), which has been around for 20 years. The country's cyber-security strategy, set up in 2011, includes a new Cyber Defence Centre and a National Cyber-Security Council to promote better cooperation between the seven federal agencies involved in cyber-security.

The current German debate is very much how to urge private companies to better protect their systems. With Berlin's plans to invest in a new smart energy grid, this is all the more urgent. As elsewhere, critical infrastructure in Germany is mostly in private hands, but the nuclear sector is suffering growing problems, and the water companies are fragmented – some are mechanical, others are IT connected. "More protection has raised the question of compensation for the investment," says Gaycken. "Or must these companies raise their prices significantly?"

Germans have painful memories of surveillance both during World War Two and in the former GDR in East Germany, so they tend to be sensitive about privacy issues. The German media is therefore very sceptical about

surveillance, and there have been public demonstrations against introducing CCTV cameras.

In 2008, the constitutional court in Karlsruhe ruled on the security versus privacy question that the security forces may only infiltrate computers with Trojan malware in very specific cases. The German hacker foundation, Chaos Computer Club (CCC), claims to have analysed spying software used by the government and come to unsettling conclusions. "This spyware was doing more than allowed," says one-time hacker **Florian Walther**, now IT Security consultant at Curesec. Discussion is ongoing among politicians and in the media.

India

India has a national CERT (CERT-in, since 2004), a crisis management plan and is setting up a Cyber Command and Control Authority. A draft of a national cyber-security policy is under discussion.

Score: ★★½☆☆

"In India, we went straight from no telephones to the latest in mobile technology," says **Cherian Samuel** of the Institute for Defence Studies and Analyses (IDSA) in New Delhi, "and the same with internet-connected computers. They came in all of a sudden, and no one was taught even the basic facts about cyber-security."

India stands fifth in the worldwide ranking of countries affected by cyber-crime, although it should be emphasised that these figures are extrapolations. Much of its vulnerability is explained by widespread computer illiteracy and easily pirated machines.

The premium on internet privacy in India is low, and data control therefore tends to be neglected. This is another reason for the success of phishing and other scams. "People in India have to understand basic security like pin numbers and passwords," says **Kamlesh Bajaj** of the Data Security Council of India (DSCI), an organisation promoting data protection. The government is taking a two-pronged approach – teaching best practices to prevent attacks, and helping capacity-building to handle incidents when attacks happen.

India is acutely aware that cyber-crime is bad for its reputation as a country where foreign investors can do business, and has been investing heavily in cyber-security. But it still lacks a single operator to control the internet, telecoms and power sectors, and even if CERT-in is the official coordinating authority, a multiplicity of other agencies are still involved.

As more and more financial service companies set up their back office operations in India, the authorities know the problem of controlling cyber-crime has to be addressed urgently. On the plus side, India has developed valuable experience in dealing with compliance regulations from around the world with the IT Amendment Act of 2008 that established strong data protection.

"These companies have a broad culture of security practices," says Bajaj. India complies, for instance, both with the U.S. and the UK's data protection acts. The DSCI is currently designing a security framework to compensate for the shortcomings of the ISO 2001 standard. It has also developed a Privacy Framework based on the international Privacy Principles.

The main challenge now for India is to train and equip its law enforcement agencies and judiciary, particularly outside big cities like Delhi, Mumbai and Bangalore. "Training and awareness must expand to cover the whole country," says Bajaj. "At DSCI, we've developed training and investigation manuals for police officers. We have trained more than 9,000 personnel of local education authorities and the judiciary on cyber-security." The programme will soon be a national programme supported by the Ministry of Home Affairs.

Israel

Israel has a national CERT, participates in the informal CERT communities, has a cyber-strategy and a cyber command.

Score: ★★★★½

"Cyber-security is not about saving information or data, but about something deeper than that," says **Isaac Ben-Israel**, senior security advisor to Prime Minister Benjamin Netanyahu, and a professor at Tel Aviv University. "It's about securing different life systems regulated by computers. In Israel, we realised this 10 years ago."

He notes that Israel sees 1,000 cyber-attacks every minute, but that there is a hierarchy of threats. "The hacktivist group Anonymous carries out lots of attacks but they don't cause much damage. The real threat is from states and major crime organisations," he says. Israel is formulating national policies to actively respond to cyber-attacks.

Last year, Ben-Israel headed a cybernetic task force that submitted recommendations to the government. Among the report's suggestions was the setting up of a cyber authority, the establishment of research centres and increased cooperation between the government, business and academia.

In 2002, Ben-Israel explains, Israel drew up list of 19 major infrastructures, including power production, water supply, banking and so on. "We faced a legal problem, how do you force the private sector infrastructure to protect themselves against cyber-attack? So we changed the laws. The level of interference of government in the private sector is a dilemma."

Nevertheless, Israel believes that the critical national infrastructure isn't adequately protected against cyber-attack. Although it is generally assumed that the Stuxnet virus that disabled the centrifuges at the Natanz nuclear plant in Iran was a joint U.S. and Israeli design, neither country has officially acknowledged this.

Israel has a building law whereby any new house or apartment has to have a room that is bomb-proof. "People accepted this law because of our experience of scud missiles in 1991. The threat was real and people felt it was real. It would have been unimaginable to establish the Patriot Act before 9/11. Once people in the street realise that terrorism is very real they accept things."

"Cyber-attacks are not just a technological problem but also legal, political and societal problems," says Ben-Israel. Following his task force's recommendations, Israel is implementing a five-year plan to place itself in the global cyber-security lead, including investment in R&D, the setting up a super-computer centre, boosting studies in cybernetics and encouraging industry to develop new technologies.

Ben-Israel claims that Israel is a model for effective collaboration between industry, defence and academia. "We have a legal framework to tell private industry what measures to take to secure the power, water and banking systems." But though he says Israel is in better shape that most countries in this area, "if you look at the threat potential there is still a lot to do."

Italy

Italy has a government CERT with insufficient funds to operate on a global scale. It takes part in cyber-incident exercises, but does not yet have a well-defined cyber-security strategy.

Score: ★★★☆☆

"Politicians in Italy tend to be more emotional than rational, and they don't understand how to measure cyber-security problems," says expert **Stefano Trumpy** of the Institute for Informatics and Telematics at Italy's National Research Council (CNR). "They need to be educated about cyber-security threats and to learn how to define them clearly."

Italy's vulnerability is still unclear. In July 2011, hackers from the group Anonymous broke into one of the country's cyber-crime units, the National Computer Crime Centre for Critical Infrastructure Protection (CNAIPIC), releasing documents about government offices in Australia and the U.S., as well as companies like Exxon Mobil and Gazprom.

The country still does not have a single body for coordinating national security, although the Ministry of Economic Development coordinates the development and implementation of the national information security strategy. In 2003, the ministries of communications, justice and internal affairs created a group to study the security and protections of networks, but this body has no legal authority.

The administration's efforts to combat cyber-threats are not uniform. Although Italy has a good contingency plan for civil protection in case of floods or earthquakes, it doesn't have one for cyber. "We lack investment that would allow general capacity building," says Trumpy. "Users and even the computer suppliers haven't been educated to protecting their machines. Most of the problems are connected to the security of personal computers used for malicious purposes."

Computer crime is reported to the Public Prosecutor (Procura della Repubblica), who directs investigations and delegates to the relevant police departments. Italy has issued laws for the protection of minors and against online gambling, but cases are rarely prosecuted.

Japan

Japan has a national CERT (JPCERT/CC), a cyber-strategy and participates in the informal CERT communities. Its cyber-security centre is the National Information Security Centre (NISC), part of the Cabinet Secretariat. In the Asia Pacific region, JPCERT/CC plays a key role in the Asia Pacific Computer Emergency Response Team (APCERT). It is a member of Forum of Incident Response and Security Teams (FIRST).

Score: ★★★½☆

In Japan, recovery from the March 2011 earthquake and tsunami remains the No.1 priority, and cyber-security is not at the top of the agenda. In the summer 2011, information systems at Mitsubishi Heavy Industry (MHI), the military equipment suppliers to Japan's Self-Defence Forces, were attacked, increasing awareness of the threat and raising cyber-security on the government's priority list. A number of measures to protect critical national infrastructure and leading industries are being put in place.

Yet funding is on the short side. "We have to put a lot of money into preparedness for natural disasters," says **Suguru Yamaguchi**, a former advisor on information security to the Japanese government and professor at the Nara Institute of Science and Technology. "As a result, the budget for defence is limited and cyber-security in not a top priority in the five-year programme to improve our defence capability." Furthermore, Japan's Self-Defence Forces are not legally in charge of protecting non-military information systems.

"Awareness raising is not enough to support the cyber-security policy agenda," says Yamaguchi. "The general public supports law enforcement for cyber-crime and capacity building of the National Policy Agency for investigations. They are not so keen on the Defence Ministry's cyber-defence programme."

"We have to put a lot of money into preparedness for natural disasters. As a result, the budget for defence is limited and cyber-security is not a top priority".

Suguru Yamaguchi

Japan is a highly wired country. Over 70% of households and over 95% of offices are connected to the internet, and mobile phones are widespread with more than 93% of people using them. In 2010, the business-to-consumer e-commerce market was estimated at about Yen 8 trillion ($100 bn). Industrial espionage targeting global firms like Sony, Panasonic, Toyota, Honda and MHI is a serious concern.

A public-private partnership (PPP) framework for cyber-protection was developed in 2006 as part of the cyber-security master plan, and so far deals with 10 critical infrastructures. "We have very good PPP in Japan," says Yamaguchi. "The government regularly updates it, and the private sector is very much involved in the discussions and processes, although dialogue could be improved further."

Good collaboration between government and industry has enabled various measures for internet hygiene. Since 2006, the malware clean-up project Cyber Clean Centre (CCC), a collaboration between ISPs and the government, has been identifying and cleaning up malware-infected PCs.

Among the hot debates in Japan is the cyber-defence role of Japan's Self-Defence Forces. The debate resembles that in the U.S, although it is unlikely that the army in Japan will work with other government agencies or the private sector, apart from the arms industry. "The debate is very complicated

in terms of legal structure, the defining of the Self Defence Force's missions and its longer-term programme," Yamaguchi explains.

The other ongoing debate involves plans to introduce an extensive ID system by 2013-15, and how to protect that system. "With fear of cyber-attacks from inside and outside Japan, what do we do to ensure citizens' privacy?" Yamaguchi asks. The programme for introducing digital IDs for all residents has launched a lively public debate involving activists, experts, government officials and law-makers.

A third issue under discussion is the role of the intelligence services in Advanced Persistent Threat (APT), or state-sponsored attacks. "Ever since World War Two, Japan's intelligence services have worked on their own. Many people in government today feel it's time for intelligence to work with other agencies."Despite this, collaboration between the different communities is good. "Government funding for cyber-security research is increasing every year," Yamaguchi says.

On the international stage, the Japan-U.S. defence alliance is effective. Japan-ASEAN hold an annual Information Security Conference, and a China-Japan-Korea (CJK) framework coordinates cyber-policy between those countries.

Mexico

Mexico does not have special rules to combat cyber-crime, but applies the existing legal framework contained in the Federal Criminal Code (or FCC).

Score: ★★☆☆☆

"In Mexico, we always face the same challenge, and that's the thin line with the physical world," says Mexican researcher **Jesus Luna** who works for the Deeds group in Germany. "If you're at an automatic cashier and a man points a gun at your head you'll give him the money, no matter what IT security measures have been adopted. A lot of problems in Mexico are related to corruption."

The Mexican government is fighting a fierce war against the drug mafia, which often has the better technology. State officials are relatively guarded about the country's cyber-strategy, and are slow in setting up regulations. "You have so many everyday challenges," says Luna. "When I was working with the central bank there, we created new technologies to try to bridge the gap between physical and technological security, and that wasn't easy."

"From a technological perspective, we could come up with solutions to cope with issues at customs at the U.S. border," says Luna, "but officials are afraid of implementing X-rays and biometrics, because they feel they would

be putting their lives at risk. People are scared of implementing security mechanisms. They don't feel protected by the government or by police and this is going to take several years to resolve."

The hackticist group Anonymous attacked several Mexican government websites in September 2011, putting them out of service intermittently over one day. The attacks were meant to highlight increased concerns about insecurity and violence. "No one took that very seriously," says Luna. "The real problem is out on the streets. Drug cartels are killing bloggers. It's that stark."

NATO

NATO's Lisbon summit in 2010 stressed the growing importance of the cyber domain for the Alliance. The Strategic Concept committed to further developing NATO's ability to prevent, detect and defend against cyber-attacks, by bringing NATO bodies under centralised cyber protection and promoting better coordination between member countries. NATO runs regular cyber exercises.

Every member of NATO's 28-member Alliance is in charge of its own cyber-security. NATO itself doesn't intervene in this area, even if according to Lithuania's Ambassador to NATO **Kestutis Jankauskas**, "every other word these days at NATO seems to be cyber." According to **Suleyman Anil**, head of its Computer Incident Response Capability Coordination Centre, NATO countries show "different levels of capability according to national resources."

NATO's modest cyber investment involves securing its own network, and identifying critical infrastructure at headquarters and agencies around Europe. In 2008, NATO set up the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, which studies incidents and techniques, and coordinates efforts between NATO members to defend against cyber-attacks and to react. NATO does not engage in global discussions about codes of conduct or international treaties. "We believe that consultation is the best deterrence," says Anil, "and that a lot can be achieved by increasing information sharing."

The Tallinn Centre's Director, Colonel **Ilmar Tamm**, believes that before creating new laws, we must first try to apply existing legal instruments to the new conditions. "For example, two bodies of international law, the *jus ad bellum* and the *jus in bello* (the latter also known as the Law of Armed Conflict), are not likely to be updated for cyber," he says. "Instead, we need to study and understand how to apply them in cases where armed conflict includes cyber-attacks." Experts on international law are working on this right now, and their research will be published as the Tallinn Manual in the second half of 2012.

NATO expects member nations to share cyber information with other members, with NATO providing communication systems support. The organisation also determines what information can be shared, and what non-member nations can know. These days, even NATO is owning up to cyber-attacks. "We were hacked

by the hacktivists of Anonymous in 2011," says **Jamie Shea**, NATO's Deputy Assistant Secretary General for Emerging Security Challenges, "and although they only got into low-level restricted documents, they got a lot of publicity out of it." NATO is reportedly considering the use of military force against nations that launch cyber-attacks against other member states, including attacks against critical infrastructure.

"The challenge was for NATO to put its money where its mouth was," says **Robert Bell**, the US Secretary of Defense's Representative to Europe, "and we're on track. We set up the Tallinn centre and our next goal is to protect critical infrastructure, the vital utilities we rely upon. NATO is also taking a lead in identifying standards that strike a balance between security and affordability." NATO will be gathering its agencies and commanders under a single cyber-defence roof by the end of 2012.

The EU is a key partner, and in recent months staff level talks have intensified. NATO looks to the EU as the regulating body and to the UN for norms of behaviour. "We have an effective level of staff discussions," says Bell. "It would be helpful if we could go beyond that and have institutional cooperation, but that's not possible because of the continuing political split between Cyprus and Turkey." NATO's main role, as Anil puts it, focuses on collective security and crisis management.

"NATO countries need to share the same standards," says Bell. "It's in part about money but not all about money." In these difficult fiscal times, NATO governments are struggling with their defence funding. As far as NATO is concerned, the compilation of cyber-incidents highlight two main problems. "The first is about outsiders trying to get in," says Bell. "The other is the workforce inadvertently putting classified information onto systems."

The Netherlands

The Netherlands has a national CERT (GOVCERT.NL), coordinates with other CERTs and is a member of the inter-governmental CERTs group (EGC). The country participates in cyber-incident exercises and has had a cyber-security strategy since 2011.

Score: ★★★★☆

The Netherlands is often cited as a cyber-security model, particularly for the exemplary relationship between the private and public sectors. Last summer, the government published a National Cyber-Security Strategy (NCSS) and installed a Cyber-Security Council to act as a platform for cyber-exchange and coordination between public sector and private companies that are part of the critical infrastructure. January 1, 2012, saw the launch of a National Security Centre.

"In the Netherlands, we've gone for a fairly bottom-up process," says **Erik Frinking**, Director of the Strategic Futures Programme at The Hague's Centre for Strategic Studies.

The attack on the certification authority DigiNotar in June 2011, most probably by Iranian hackers, pushed cyber up on the political agenda. As a result of the attack, DigiNotar lost its biggest client, the Dutch government, and filed for bankruptcy three months later.

"Our problem is that we are all reinventing the wheel"

Elly Plooij-Van Gorsel

Elly Plooij-Van Gorsel, Founding Chair of the European Internet Foundation (EIF), former Vice-President of the European Parliament and member of the Governmental International Advisory Council (AIV), was one of the authors of an advisory report to the government on cyber-security in foreign affairs, security and defense policy, published in January 2012, that demands an international code of conduct, and better information sharing at both civilian and military levels.

"The question is how far as a state can you intervene? What are the threats? How real are they?", she asks. "We need good early warning systems, good intelligence and much better information sharing. Our problem is that we are all reinventing the wheel, and that's the big impediment to global security. Cyber-attacks are borderless, so we have to cooperate and coordinate, starting within the EU."

The new cyber-security strategy is also under debate, says Frinking. "Everyone agrees it's not really a strategy," he says, "but more a short-term action plan with a combination of activities that seem important right now. It lacks an overall framework and a more conceptual idea of what is going on."

Despite its effective public-private partnership, the Netherlands has a number of weaknesses. One is that cyber-security is fairly decentralised. "We need better coordination for a more focussed approach," says Frinking. "At present, the money is shared out between too many different departments."

Frinking also considers a lack of international outlook as another Dutch weakness, even if this is shared by most countries. "A lot still needs to be accomplished at multilateral and international levels, and in EU forums. If something happens at national level that comes from foreign sources, how does the government position itself? Who does it call upon? What interests does it want to defend? We don't really know."

On the balance between security and privacy, Frinking says the hardest debate is still to come. "We've organised discussions on this issue at our institute to try to think differently about privacy. These are not good days for privacy proponents. They are put aside fairly quickly in the debate." The urgent issue, he says, is to raise awareness with the common users. "I am flabbergasted by the naivety of some people on the internet, although we are seeing more and more public campaigns to change that."

Poland

Poland has a national CERT (CERT.Polska) and a government CERT (CERT.gov.pl). It takes part in the informal CERT community and in cyber exercises, but does not yet have a cyber-security strategy.

Polish analysts say the country's younger generation is increasingly connected, and that Poland can claim to be the most technologically advanced country in Central Europe. "Much yet needs to be improved," says **Janusz Gorski**, head of the software engineering department at the University of Gdansk, "but the debate has started."

The CERT community is well developed across the country, with responsibility for fighting cyber threats in the hands of the government CERT. A cyber-strategy is currently being set up. The national and government CERTs use an early-warning system that doesn't have access to private data because the sensors are installed outside the private networks. Many Poles are concerned with the rapid growth in internet financial crime. In the first half of 2010, law enforcers initiated 881 proceedings: by 2011, that figure had jumped to 1,220.

Gorski feels strongly, however, that Poland lacks public awareness and education. Young people aren't choosing to study cyber-security. "Students are interested in the subject," says Gorski, "but they don't see a career in it." As in most countries, funding is insufficient and the economic crisis isn't helping.

The debate, Gorski believes, is based more on scare stories in the media than hard facts or good communication between the technological people and decision-makers. The public-private partnership is not strong and is hindered, in Gorski's words, by "a great deal of corruption."

As in other central European countries, citizens feel strongly about privacy issues. "People here are keen on their privacy but they don't yet see the connection with cyber-security," explains Gorski. "They don't know how much data is in the public space."

Poland is an active player in international exercises. In 2010, the country participated in Cyber Europe 2010, the first pan-European exercise on the protection of critical information infrastructure. Poland also took part in the 13th Nato Cyber Workshop in Tallinn in 2010.

Romania

Romania has a national CERT, takes part in informal and formal CERT groups, has a cyber-security strategy, and engages in cyber-exercises.

Score: ★★½☆☆

Romania has been rapidly catching up on the cyber-security front. Where, not long ago, the country was a haven for cyber-criminals because of a lack of legislation, now the police has been doing a good job at getting things under control. In 2011, cyber-crime prosecutor Ioana Albani was awarded the title of Prosecutor of the Year for the number of arrests and prosecutions she successfully conducted.

"We've been there before, we know how bad it is when governments intercept calls and communications"

Aurel Sima

Nonetheless, resources are scarce and awareness among the common user is low, says **Aurel Sima**, a cyber-security expert who has been carrying out an extensive audit on his country's critical national infrastructure. The European Union has been funding a number of cyber-security infrastructure-building projects in Romania, which should see an improvement in the situation within the next five years, but the public-private partnership is still immature. The government is planning to implement a nation-wide cyber-security policy.

EADS is planning to open two competence centres in 2012, one for cryptography and the other for cyber-security. IBM is opening a systems laboratory in Bucharest, the first European site for developing IBM switches and networking hardware and software, and Hewlett Packard has plans for a security development facility. The reason, says Sima, is that Romania scores high on technical knowhow. The state encourages IT development, with a 10-year-old policy of tax breaks for companies that hire internet programmers. "A lot of well trained Romanians have worked abroad for Google, Yahoo and others, and they're coming back with lots of expertise, having earned the trust of big companies."

Romania is among the top 10 countries for broadband internet speed, and more and more people are using the internet. Sima says this is partly explained by the high level of emigration. "Three million Romanians work abroad," he says, "and the internet is an affordable way for them to stay in touch with people back home. This has greatly helped internet penetration."

After years of dictatorship, Romanians love their privacy. "We've been there before," says Sima. "We know how bad it is when governments intercept calls and communication. This is why the government is trying to find ways to protect the confidentiality of communication and data transmission." Romania is working with law enforcement agencies in the EU and the U.S., and has a structured system for cyber-security cooperation with NATO.

Russia

Russia has a national CERT (ruCERT) that participates in the informal CERT communities and is a member of FIRST. It issued strategic guidelines in 2011. The Security Council of the Russian Federation coordinates the four ministries in charge of cyber-security (Interior, Justice, Foreign Affairs and Defence).

Score: ★★★☆☆

It's difficult to sort the wheat from the chaff when writing about Russia and trying to distinguish between popular Western prejudices and governments' concerns about Russian cyber-practices. In its October 2011 report to the Congress, the US Office of the National Counterintelligence Executive openly accused Russia and China of cyber-espionage that represents "a persistent threat to U.S. economic security." In the words of one expert, Russia is "a thug state with great hackers."

Vladimir Chizhov, the Russian Federation's Ambassador to the EU, stresses Russia's campaign for an international cyber arms-control agreement. Russia, along with China, belongs to the Shanghai Cooperation Organisation (SCO), whose members signed a code of conduct in cyber-space.

Acts of terrorism are a major concern in Russia, as is social networking that could unsettle the regime and bring about a "Russian Spring". "We've been a target of terrorist attacks," says Chizhov, "and as technology develops we can't disregard cyber-terrorism. But we need to take the international route, starting with an international codification of the terms cyber-attack, cyber-crime and so on. This type of crime can only be successfully fought through international cooperation, and we believe the UN is the right venue."

"This type of crime can only be successfully fought through international cooperation, and we believe the UN is the right venue"

Vladimir Chizhov

Vitaly Kamluk is a technical expert at Kaspersky Lab and well versed in Russian cyber-crime. "Russia is known around the world for certain types of attacks," he explains. "Top among them are banking trojans and spam-sending botnets. But we're growing more and more like the rest of the world now. What's new is that Russian hackers are now targeting local citizens, which they didn't before."

In Russia, unlike other large countries, you can still register a service anonymously. "There's no open debate on the subject," says Kamluk. "The money stays at companies that provide legal services for short premium SMS numbers, which suits businesses. But it also suits cyber-criminals." According to Kamluk, where Russia is more open than most countries in the West is on internet forum debates. "My experience is that there are a lot of beginners out there discussing things very publicly. It's quite easy to join and monitor the activities of cyber-criminals."

Russia is tightening up its defences against home-grown cyber-crime, with new regulations on the security of private data, on protecting digital signatures and on the registration of domain names, which until recently could be set up without verification. Chizhov says he hopes the public-private partnerships in Russia are working "reasonably well", and believes that private companies are aware of the risks posed by cyber-crime.

Large swathes of the country are not yet connected, which makes Russia less dependent on its critical national infrastructure than other countries. "It's a huge territory," says **Alexey Salnikov**, Vice Director of Information Security at Lomonosov Moscow University, "and the internet is not involved in all the structures of government. In Siberia, for instance, there is very little internet connection. We have a lot of intranet compared to the U.S. and Europe."

Despite Russia's reputation for technological know-how, Salnikov says they urgently need more researchers. "We have some 100 institutes and universities that deliver courses for future specialists of information security, but that's not nearly enough."

Spain

Spain has a government CERT and takes part in the informal CERT community and the national CERTs in the EGC group, but doesn't yet have a cyber-strategy. It takes part in cyber-incident exercises. The National Intelligence Service (CNI) heads the National Security Scheme/Esquema Nacional de Seguridad (ENS) that establishes minimum security requirements and protective measures to be met by administrations.

Score: ★★★★★

"Cyber defence spending must be increased," says Spanish intelligence chief **Felix Sanz Roldan**. ICT spending on government systems rose until 2008, but has either remained the same or been cut since then. "The threat of state-sponsored cyber-attack is real and one of the most serious that confronts Spain's information systems," says Sanz Roldan.

Back in 2009, members of the Senate began urging the government to speed up its implementation of a national cyber-security plan. With the new government elected in November 2011, and the economic crisis the top priority, it remains to be seen how quickly action will be taken.

"The threat of state-sponsored cyber-attack is real"

Felix Sanz Roldan

Spain has a national public prosecutor for cyber-crime, as do some of its autonomous regions. The country also has national CERTs, and some regions like Valencia have their own CERTs, but there is no single body under a single national policy. So far, the CCN-CERT (the national intelligence's CERT) is filling this role, including the protection of national critical infrastructure.

"We urgently need to coordinate at all government levels," says Colonel **Emilio Sanchez De Rojas**, cyber expert at the Ministry of Defence, "and at the European and global levels. The government needs to invest but so does private business, and we need to coordinate the two."

In its electoral programme, the governing centre-right Popular Party contemplated a national coordinating authority on security, including cyber. In the meantime, ENS has established three levels of security requirements for usage and tools – low, medium and high. When the national cyber-

security strategy is in force, these ENS requirements will be applied to the private sector's critical infrastructure.

Sweden

Sweden has a national CERT (CERT-se) that is a member of the EGC Group, and that takes part in informal CERT communities. It has a national cyber-security strategy, a national plan for cyber-incidents and organises and participates in cyber-exercises.

Score: ★★★★½

"Our awareness has been greatly raised over the last five years. We no longer have low-hanging fruit to be picked off," says **Lars Nicander**, director of the Centre for Asymmetric Threat Studies (CATS). "Security is growing tougher and tougher, and although there will always be loopholes, you would have to be very knowledgeable to effect an intrusion."

The Swedish Civil Contingencies Agency (MSB) supports and coordinates information security across society, from local municipalities to national critical infrastructure operators. MSB hosts a cooperation group for information security (including the armed forces and the post and telecom agencies, among others), as well as the country's national CERT.

MSB reports to the Ministry of Defence, but four cabinet departments are in fact involved in cyber-security (defence; enterprise and industry; foreign affairs; justice). "That's too much," says Nicander. "We need a top-down approach to cyber norms to establish who owns them, and a bottom-up approach to carry out technical cyber-defence exercises."

As Director General of MSB, **Helena Lindberg** says her agency's task is to assess risks and vulnerabilities, raise awareness, coordinate stakeholders and create networks. "What's unique to Sweden," Lindberg says, is that "we don't box things in. We're good at cross-sectoral work and involving all stakeholders."

Work is being done to improve the public-private partnership, however, which is generally thought not strong enough. "We need the expertise of private companies," Lindberg says. 'They know more about technological developments and they know their own vulnerabilities.'

Sweden scores well on technical exercises, although the country's top decision-makers lack cyber knowledge. As elsewhere, the gap between the technical people and the policy-makers needs to be closed.

"Cyber-security isn't just about more sophisticated technology and more money," Lindberg says. "It is also a 'people' problem. We need better governance at all levels of society and we need to get the best brains working on this."

"We need better governance at all levels of society and we need to get the best brains working on this"

Helena Lindberg

"Sweden plays a leading role among Nordic countries both at the innovation level and in helping other countries work together," says **Roger Forsberg**, chief information officer for the Swedish Fortifications Agency (SFA), which manages public defence related buildings and land.

"We're lucky in having a defence heritage from the Cold War," says Nicander, "when we spent lot of money on redundancies in critical infrastructure. We're not as vulnerable as the US was in the mid-90s when their SCADA systems had no protection at all." Cyber-security of industrial control systems (SCADA) is a hot topic in Sweden as elsewhere, and the MSB and the Swedish Defence Research Agency have built a capacity laboratory for the cyber-security of SCADA systems.

United Kingdom

The UK has an Office of Cyber-Security and Information Assurance (OCSIA) and a Cyber-security Operations Centre (CSOC). The former is based in the Cabinet Office and the latter is located within GCHQ, the UK's electronic intelligence agency. The UK has a national and a government CERT, takes part in the informal CERT community as well as the EGC Group of inter-governmental CERTs. In 2011, it updated its cyber-security strategy and takes part regularly in cyber-incident exercises.

Score: ★★★★☆

The UK published its updated cyber-strategy in November 2011. "The 2009 version was out of date," says **Fred Piper**, cryptologist and founder of the Royal Holloway Information Security Group. "The theme now is that the internet is here to stay. We need it for industry, governments and individuals and we must make it secure. The previous approach was more about fear, uncertainty and doubt."

The government has assigned a four-year budget of £650m to cyber-security, including establishing norms of good behaviour in cyber-space. The new strategy promises that the new National Crime Agency is to have a cyber-crime arm by 2013, and more resources are to go towards law enforcement on cyber-crime with a Home Office Cyber-Crime Strategy to be reviewed every six months.

"There are many good ideas within the policy document," says information-security expert **Peter Sommer**. "OSCIA has gone out of its way to consult widely, but there are also problems that will need to be addressed. How will these plans be put in action? There are no plans for a UK cyber tsar. Then, a great deal depends on cooperation from the private sector, which controls about 80% of the critical national infrastructure. Finally, over half of the new funding will go to the 'secret vote', the intelligence agencies, where value for money will be difficult to investigate. I would have preferred more emphasis on public education – helping potential victims help themselves."

In 2011, child benefit data on two computer discs was famously lost. That incident made the British public more aware of the "human factor" in cyber-security. "There is a swing away from regarding cyber-security as a purely technological issue," says Piper, "A lot more effort now is going into things like awareness programmes and educating the citizens to look after their own computers." A public website, GetSafeOnline, is specifically addressed to ordinary users.

One feature of UK culture, according to Sommer, is that "much discussion in the UK takes place out of the public gaze. MI5 and the intelligence agencies set up informal meetings where people get to know each other and share concerns, but it's kept below the public horizon. People are more candid away from the full glare of public scrutiny."

The government's approach, says Sommer, has been to avoid imposing regulations and thus setting things in stone. "They'll have to impose regulations to ensure that adequate preventative and recovery measures are in place," he says. "The main problem is how do governments interact with large commercial businesses in this relatively new situation?"

The UK government has been talking to the major infrastructure companies since the late 1990s, when alarm bells were ringing over fears about the "millennium bug". One hope is that these relations can be formalised via an information exchange "hub".

The one problem, Sommer says, is a failure to understand the limitations of the public-private partnership. "The fact is that private companies owe their first obligation to their shareholders, and many of the UK's leading utilities companies are substantially owned by overseas companies, such as Germany's Eon and France's EDF."

UNITED NATIONS

Many see the UN as the ideal conduit for fostering relationships between nations and promoting discussions on cyber-threats. **Hamadoun Touré**, the International Telecommunications Union's Secretary General (ITU) believes that a global treaty could include an agreement that countries protect their citizens in the case of cyber-attack, and agree not to harbour cyber terrorists.

Russia and China would like to see this UN treaty. The U.S. and the UK, on the other hand, prefer the Budapest Convention on Cyber-Crime introduced by the Council of Europe in 2001, and argue that the UN institution is too slow and cumbersome. The Budapest Convention, which has been ratified by 120 countries, is used by prosecutors to secure electronic evidence of cross-border crime.

UNESCO is another UN agency involved in the cyber-space debate, focussing on the protection of Article 19 in the Declaration of Human Rights which guarantees freedom of expression. "Article 19 is an enabler of other rights," says **Andrea Beccalli**, an ICT specialist who has designed policies for UNESCO. "We try to stress this to our member states, particularly the right to assembly. Shutting down a blog or a Facebook page is a violation of Article 19. The right to assemble and discuss in cyber-space also comes under Article 19."

UNESCO considers access to the internet as every person's basic human right, and that when designing national cyber-security agendas, countries must make sure citizens are aware of their rights on the internet, as well as the internet's threats and potentials. "Our position is that training can teach individuals to protect themselves," says Beccalli. "UNESCO is basically promoting a multi-stakeholder approach that goes beyond the constituency of member states and accredited private sector parties."

Beccalli says one of the big upcoming debates in cyber-space is who will be in charge of the governance of smart phones. Smart phones are spreading rapidly through Africa, with 99% of new internet connections in Kenya done by young people using mobiles. "We need an established model that is nimble enough to keep the constituency open and the debate as broad as possible for all actors and stakeholders. We want to make use of these technologies, while moving towards a policy development process totally different from that done by inter-governmental organisations, which is too stiff and not inclusive enough to see where these new technologies and applications are going."

United States of America

The U.S. has a government CERT, takes part in the informal CERT communities, and has a new cyber-security strategy since 2011. It has a contingency plan for cyber-incidents and is an active player in cyber-security exercises. The Pentagon has a cyber-command (USCYBERCOM) that defends American military networks and can attack other countries' systems.

Score: ★★★★☆

"From my perspective, there's never been a cyber-attack on the U.S., but countless episodes of espionage and crime, "says **James Lewis**, senior cyber expert at the Center for Strategic and International Studies (CSIS).

Kevin Gronberg agrees with him. The senior counsel for the House of Representatives Homeland Security Committee, says: "The term cyber war is as unhelpful as the expression Cyber Pearl Harbour or Cyber 9/11. It's what internet people call fear, uncertainty and doubt. We need nuance because this issue is complex and touches on so many elements of our economy and way of life."

The naming of a White House cyber coordinator, known as the Cyber Tsar, in 2011 has moved the U.S. away from what Lewis once described as a "tribal approach", in which too many players held the field.

"From my perspective, there's never been a cyber-attack on the U.S., but countless episodes of espionage and crime"

James Lewis

"It's an important position to help coordinate throughout government," says **Melissa Hathaway**, a consultant in Washington, DC, who led President Obama's Policy review, "but the position is not ranked high enough in the White House structure to have the authority needed to drive change."

The November 2011 strategic guidelines on cyber-security add up to a well-thought-out document, says Lewis, that is deliberately not set in stone. "The day after the guidelines were realised," he says, "the Department of Defense held a small meeting with experts. The first thing they said is that they were already working on the next version."

Lewis says the guidelines have been widely misinterpreted, for instance on the issue of when to use deterrence, or when and how to use offensive

capabilities for defensive purposes. "Threatening military retaliation for malicious action in cyber-space makes sense to prevent attacks," he says, "but it doesn't work against espionage or crime because neither of them involve the use of force. So it doesn't apply in many cases."

And it's the exploitation of the internet by strategic competitors that is most damaging to the U.S. and Europe. "China and Russia are the most active," he says, "but China is noisier than Russia." Does the U.S. itself indulge in cyber-espionage? No, says Lewis, and for two reasons. "For one thing, our laws don't allow us to favour one company over another, so would we be spying for Boeing, or who? Secondly, until recently they didn't have much in way of technology we would want to steal." Rather than designing an international cyber-security treaty, the U.S. favours improved collaboration with international law enforcement agencies.

How good is public-private partnership in the U.S.? The Department of Defense has a solid relationship with the defence industrial base, says Gronberg. Lockheed Martin, for instance, has developed a legal framework for sharing cyber-security information with other companies. "This hasn't been the silver bullet that solves all problems," says Gronberg, "but it has gone a long way to improving levels of trust in that sector and it's the most innovative cyber-security development of the last five years." The model could be expanded to the other utilities like the power grid and financial service sectors, among others.

But there are barriers that don't make this easy to do. Gronberg blames the laws that limit information sharing. "We need to address this problem in Congress," he says, "but Congress moves extremely slowly. We need government and the private sector to work together better, faster and across more sectors." Others believe the relationship is a "big brother-little brother one, rather than a partnership of equals", adding "in the U.S., we struggle with the idea of trusting government."

Among the hottest cyber-security debates, says Hathaway, is the extent to which the U.S. government is considering regulating industry. "Industry is unhappy with regulation on a lot of levels," says Hathaway, "including costs." On the balance between security and privacy, she thinks the privacy advocates will win every time. "But a lot more could be done to protect privacy while enhancing our security posture," she says. "They don't have to be opposing forces. They could work in tandem. This requires updating some of our laws, and having a robust dialogue about what needs to be overhauled when the threat and technology are constantly changing."

"A lot more could be done to protect privacy while enhancing our security posture"

Melissa Hathaway

Among interesting experiments at state level is that carried out by the public affairs firm Resolute Consulting, which set up a 12-member task force to look at what Illinois should do to protect its critical infrastructure from cyber-attack. "Data in Illinois was all over the place, and we worked on how to secure networks and increase resiliency," says Resolute Consulting Vice President **Jake Braun**. They hope to do similar work in other states.

The U.S. is engaging primarily at a bilateral level, which is always easier than broader, multi-state international engagement, says Hathaway. "But in order to make a difference, all countries have to take responsibility for what's happening in their own infrastructure, and the only way to achieve that is through international organisations. We have to agree in the G20, NATO and the UN about what is acceptable."

"No one owns the internet," another senior American says, "not even the U.S. As such, engaging in a hegemonistic relationship with another sovereign nation is not the way to go. We need to share our expertise with allies no matter what the issue, energy production, cyber-security or defence tactics, and that should go both ways. All boats float on a rising tide."

INDICES AND GLOSSARIES

Cyber sources

Contributors to this report

Mohd Noor Amin is the Chairman of the International Multilateral Partnership Against Cyber Threats (IMPACT), a United Nations-backed public-private partnership. With 137 partner countries, IMPACT has become the largest cyber-security alliance of its kind.

Suleyman Anil is Head of Office at the NATO Computer Incident Response Capability Coordination Centre (NCIRC - CC). He has over 20 years experience in information-security and cyber-security with NATO.

Frank Asbeck is Principal Counsellor for Security and Space Policy for the European External Action Service.

Ioannis G. Askoxylakis is Coordinator of FORTHcert in Greece that provides computer security incident response for the Foundation for Research and Technology - Hellas.

Victoria Baines is a strategic analyst for the European Police Office (Europol), where she is responsible for developing strategies to combat cybercrime.

Kamlesh Bajaj is CEO of the Data Security Council of India (DSCI) and was founding Director of the Indian Computer Emergency Response Team (CERT-In) at the Ministry of Communications and IT.

Judy Baker is Director of Cyber Security Challenge UK Ltd. Previously, she helped set up the UK Government's National Infrastructure Security Coordination Centre (NISCC) and the Centre for the Protection of National Infrastructure (CPNI).

Stewart Baker is a Partner at Steptoe & Johnson in the U.S. He served as Assistant Secretary for Policy at the Department of Homeland Security, with responsibility for international and policy issues relating to cyber-security, and as General Counsel of the National Security Agency.

Andrea Beccalli is an Associate Expert at the Information Society Division of UNESCO and has extensive experience in the field of Information and Communication Technology (ICT) for development, international communication and information policies.

William Beer is a Director in Pricewaterhousecooper's (PwC) Cyber and Information Security practice in London and works with clients to develop solutions for cyber-related matters combining computer forensics, data analysis, malware analysis, cyber-surveillance and crisis management.

Robert G. Bell is the Senior Civilian Representative of the U.S. Secretary of Defense in Europe. He is responsible for planning, recommending, coordinating and monitoring Department of Defense (DoD) policies, programmes and initiatives throughout Europe.

Isaac Ben-Israel is Chairman of the Israel National Council for Research and Development and the Israel Space Agency. He led a team that submitted recommendations to the Israeli government on how to prepare for the threat of cyber-attack, and was the Senior Cyber-Security Advisor to the Israeli Prime Minister.

Gorazd Božič is the Head of the Academic and Research Network of (ARNES) CERT in Slovenia and a member of the ENISA management board.

Jake Braun is Executive Vice-President at Resolute Consulting in Chicago. His responsibilities include designing and implementing public affairs campaigns focusing on the firm's homeland and cyber-security practice.

Vytautas Butrimas is Chief Advisor for Cyber-Security at the Lithuanian Ministry of Defence, having worked in information technology and communications for over 20 years.

Oliver Caleff is CSIRT Manager at CERT-DEVOTEAM in France and is a senior security consultant with experience in IT and other fields of security.

Vladimir Chizhov is Permanent Representative of the Russian Federation to the EU. A former Deputy Minister of Foreign Affairs, he has extensive knowledge of cyber-security issues and their impact on international security.

Larry Collins is Vice-President for e-solutions at Zurich Financial Service where he develops and delivers on-line cyber risk prevention tools.

Richard Crowell is an Associate Professor of joint military operations at the U.S. Naval War College. Additionally, he serves as the College of Naval Warfare coordinator for contemporary operating environments.

Ed Dawson is Senior Advisor at the Information Security Institute at Queensland University, Australia. He has written more then 200 papers on cryptology and has been involved in projects related to secure electronic commerce and mobile communications.

Freddy Dezeure is Head of the Inter-institutional Computer Emergency Response Pre-Configuration Team for European Union institutions (CERT-EU).

Jean-Michel Doan is a cyber-crime analyst at Lexsi Innovative Security.

Roger Forsberg is Chief Information Security Officer for the Swedish Fortifications Agency under the Swedish Ministry of Finance. He is responsible for securing government-owned defence related buildings from cyber-threats.

Erik Frinking is Director of the Strategic Futures Programme at The Hague Centre for Strategic Studies (HCSS). He played an important role in the development and implementation of the Dutch National Security Strategy.

Nick Galletto is the National Leader for Information & Technology Risk for Deloitte in Canada. He has over 20 years experience in information technology, networking and systems management and the implementation of information technology solutions.

Sandro Gaycken is a researcher and professor of cyber-security at the Institute of Computer Science at the Freie Universität Berlin, Germany.

Thierry Gobillon is an Information Security Officer, Risk Management & Compliance for ING bank in Brussels, Belgium. His role requires him to secure banking information from cyber-threats.

Janusz Górski is Professor of Software Engineering at the Faculty of Electronics, Telecommunications and Informatics at Gdansk University of Technology in Poland.

Peter Gridling is the Director of the Federal Agency for State Protection and Counter Terrorism in the Austrian Ministry of Interior.

Kevin Gronberg is Senior Council on cyber-security issues to the United States House of Representatives, committee on Homeland Security. He was the legal counsel to DHS's US-CERT.

Timo Härkönen is Director of Government Security for the Office of the Prime Minister in Finland. His responsibilities include security planning, preparedness planning and crisis management at government level.

Melissa Hathaway is President of Hathaway Global Strategies, an independent consultancy based in the U.S. She served in the Obama Administration as Acting Senior Director for Cyberspace at the National Security Council and led the Cyberspace Policy Review.

Jun Inoue is First Secretary and Telecom Attaché at the Mission of Japan to the EU.

Timothy Jordan is a Senior Lecturer at Kings College University in London. His areas of expertise include internet studies, hacking and hacktivism.

Vitaly Kamluk is chief malware expert at Kaspersky Labs in Russia and specialises in threats to global network infrastructures, malware reverse engineering and cyber-crime investigations.

Alexander Klimburg is a Fellow and Senior Advisor at the Austrian Institute of International Affairs. He has published widely on the subject of national cyber-security and is the principle author of a commissioned study to the European Parliament entitled "Cyber-power and Cyber-security"

Robert F. Lentz is President and CEO of Cyber Security Strategies, LLC and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance (CIIA) in the Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer.

James Lewis is a Senior Fellow and Director of the Technology and Public Policy Programme at CSIS, where he focuses on national security and the international economy.

Herbert Lin is chief scientist at the Computer Science and Telecommunications Board of the National Research Council (NRC) of the National Academies in the U.S. He has directed several studies on cyber-security issues.

Helena Lindberg is Director General of the Swedish Civil Contingencies Agency and is responsible for unifying, coordinating, and supporting tasks in preparation for, during and after emergencies, including those related to cyber-security.

Jesus Luna is a researcher for The Deeds group in Germany. His areas of expertise include security metrics, cloud and grid security, botnet mitigation, security and privacy.

Alastair MacWillson is Global Managing Director of Accenture's Global Security practice. He has been adviser to a number of governments on technology strategy, critical infrastructure protection, cyber-security and counter-terrorism.

Raphael Mandarino Jr. is Director of the Institutional Security Cabinet for the Department of Information Security and Communications in Brazil. He has extensive experience in the coordination efforts of national CSIRT and their law enforcement agencies.

Dave Marcus is Director of Security Research for McAfee Labs. He has extensive experience in network solutions and IT security, with a focus on advanced intelligence gathering, digital forensics, intrusion detection and prevention, and network and host analysis.

Marina Martinez-Garcia is Programme Officer at the Centre for Industrial Technological Development (CDTI) in Spain and is responsible for fostering Spanish science and technology participation and assistance at the EU level.

John I. Meakin is Director of Digital Security and CISO of BP. He is a specialist in information systems security with more than 20 years experience.

Lars Nicander is Director of the Centre for Asymmetric Threat and Terrorism Studies (CATS) at the Swedish National Defence College (SNDC).

Satoshi Noritake is the Senior Manager, Certified Information Systems Security Professional (CISSP) for NTT Communications Corporation.

Andres Ortega is the former Director General of the Department of Analysis and Research in the Spanish Prime Minister's Office. He was responsible for analysing information on cyber-security threats.

Evangelos Ouzounis is Head of Resilience and Critical Information Infrastructure Protection Unit of ENISA.

Patrick Pailloux is Director General of France's Network and Information Security Agency (ANSSI). He is responsible for all matters related to cyber-security in the French government.

Fred Piper was the founding Director of the Royal Holloway Information Security group, a member of the permanent stakeholder group at ENISA and a member of the International Advisory Board of the International Multilateral Partnership Against Cyber Threats (IMPACT).

Elly Plooij-Van Gorsel is a member of the International Advisory Council (AIV) where she advises the Dutch government and parliament on foreign affairs and defence including cyber-security.

Jaan Priisalu is the Director General of the Estonian Information Systems Authority and was head of IT Risk Management at Swedbank. His responsibilities include the oversight and protection of Estonia's critical public and private information systems.

Steve Purser is Head of ENISA's Technical Competence Department where he is responsible for agreeing the annual work programme with stakeholders and ensuring that this work programme is successfully implemented.

Gerrard Quille is a foreign, security and defence expert at the Directorate-General for External Policies of the European Parliament. He has been involved in various projects relating to cyber-security.

Costin Raiu is Director for Global Research and Analysis at Kaspersky Lab and specialises in malicious websites, browser security and exploits, e-banking malware, enterprise-level security and Web 2.0 threats.

Christopher Richardson is a research engineer and lecturer at the Ministry of Defence College in the UK. He focuses on information risk management and network security management in the military and NATO and is developing system and traffic analysis and simulation of MoD deployed CIS.

Rafal Rohozinski is the founder and CEO of the SecDev Group and Psiphon Inc. He is also a Senior Fellow at the Munk School of Global Affairs of the University of Toronto. His work in information security spans two decades and 37 countries, including conflict zones.

Alexey Salnikov is Vice-Director Institute of Information Security at Lomonosov Moscow University. He specialises in discrete mathematics, cyber-terrorism, political and humanitarian issues of information security and international cyber-policy.

Cherian Samuel is Associate Fellow at the Institute for Defence Studies and Analyses in India. He is an expert in Indo-U.S. relations and has written on Indian cyber-security and Indo-U.S. cooperation on cyber-security issues.

Emillo Sanchez De Rojas is Head of Department of Strategy and International Relations at the Centre for National Defence Studies in Spain where he also advises on cyber-security policy and strategy.

Felix Sans Roldan is Director of the National Intelligence Centre in Spain. He is also responsible for the National Cryptological Centre and oversees Spanish cyber-intelligence and defence.

Phyllis Schneck is Vice-President and Chief Technology Officer, Global Public Sector at McAfee.

Tim Scully is CEO of Stratsec and Head of Cyber Security at BAE Systems Australia. He has extensive experience building and leading intelligence and security capabilities and teams in the Department of Defence.

Andrea Servida is Deputy Head of Unit for Internet, Network and Information Security in the Directorate-General for Information Society and Media of the European Commission.

Jamie Shea is the Deputy Assistant Secretary General for Emerging Security Challenges at NATO.

Aurel Sima is a Security Auditor for Genos Consulting in Romania and is responsible for securing data centres and databases and providing security training to clients.

Bart Smedt is a Research Fellow at the Belgian Royal Higher Institute for Defence. His areas of expertise cover proliferation issues, critical infrastructure protection, cyber-defence and emergency planning.

Peter Sommer is a reader at the UK's Open University and a former Visiting Professor at the London School of Economics specialised in computer security and cyber-threats.

Tim Stapleton is Assistant Vice-President and Professional Liability Product Manager for Zurich North America.

Ilmar Tamm is Director of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.

Brooks Tigner is the Editor of Security Europe in Brussels. He has reported on security and defence issues across Europe for many years.

Heli Tiirma-Klaar is Senior Advisor to the Undersecretary of Defence in Estonia. She led the working group that developed the Estonian Cyber-security Strategy in 2008.

Hamadoun Touré is Secretary General of the International Telecommunication Union (ITU).

Stefano Trumpy is Research Manager at the Institute for Informatics and Telematics of the Italian National Research Council and the Italian delegate in the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN).

Jüri Vain is Director of the Department of Computer Science at Tallinn University of Technology. His main areas of expertise are deductive verification, model-based testing and model checking.

Wouter Vlegels is Critical Information Infrastructure Protection expert at ENISA and has a particular interest in the interrelationships and information sharing between NATO the national authorities in the capitals of member nations and the EU.

Florian Walther is a senior IT security consultant at Curesec consulting in Germany. He is an active member of the German hacker community and has spoken at the Chaos Computer Congress, SigInt and ph-neutral.

Peiran Wang is a PhD Candidate at East China Normal University's School of Advanced International and Area Studies and a visiting researcher at the Vrije Universiteit Brussels (VUB). His areas of research include international security and cyber-security.

Christian Wernberg-Tougaard is a member of the Information Security Advisory Board at the Ministry of Science, Technology and Innovation in Denmark and a member of ENISA Permanent Stakeholders Group. He provides advice on information security to the Danish government.

Suguru Yamaguchi is a Professor at the Graduate School of Information Science at Nara Institute of Science and Technology in Japan and a former Advisor on Information Security to the Cabinet of the government.

Takeo Yoshida is the Deputy director of the Ministry of Internal affairs and Communications (MIC) in Japan. He is responsible for advising and formulating policy and strategy on Japan's cyber-defence and cyber-security protocols.

Glossary of organisations

Asia-Pacific Economic Cooperation (APEC) - Telecommunications and Information Working Group (TEL)

Where: Singapore

Funding: Member economies: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Singapore, Russia, Taiwan, Thailand, U.S., Vietnam

Mission: APEC's TEL aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing telecommunications and information policies. The four subgroups within TEL are the Security and Prosperity Steering Group (SPSG), the ICT Development Steering Group (ICTDSG), APEC-TEL MRA and the Liberalisation Steering Group. The SPSG and ICTDSG are of particular importance to cyber-security in Asia. The SPSG's responsibilities include cyber-crime prevention and promoting security and trust in networks, e-commerce and infrastructures. ICTDSG promotes ICT applications to socio-economic developments such as smart grids, crisis management and advanced technologies.

Website: http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx

Email: info@apec.org

Association of South East Asian Nations (ASEAN) - Telecommunication and IT (TELMIN)

Where: Jakarta, Indonesia

Funding: Member economies: Brunei, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Vietnam

Mission: TELMIN is a sub-grouping of ASEAN. Its mission is to develop a common framework to coordinate exchange of information, establishment of standards and cooperation among enforcement agencies. Part of the TELMIN annual programme includes sessions with the ASEAN Dialogue Partners on a Plus Three basis (with the People's Republic of China, Japan and the Republic of Korea) and a Plus One basis (with India). TELMIN also engages with the telecommunications and IT industry players in ASEAN through the e-ASEAN Business Council comprising representatives of the private sector from all ASEAN member countries.

Website: http://www.aseansec.org/19594.htm

Council of Europe

Where: Strasbourg, France

Funding: Its 47 member states

Mission: The Council of Europe provides three mechanisms: 1) 'Cooperation against cyber-crime' which aims to establish a global framework for efficient cooperation against cyber-crime, 2) the 'Cybercrime Convention Committee' which support the strengthening of legislation and capacity building, and 3) the 'Contact points for police and judicial cooperation' which facilitates the implementation of the Budapest Convention on Cyber-crime.

Website: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp

Email: cybercrime@coe.int

Commonwealth Telecommunications Organisation (CTO)

Where: London, United Kingdom

Funding: Members of the Commonwealth of Nations

Mission: The CTO is an international development partnership between the Commonwealth and non-Commonwealth governments, business and civil society organisations. It promotes social and economic development in the Commonwealth and beyond, helping to bridge the digital divide by facilitating the development of telecommunications among developing member states and to achieve the Millennium Development Goals for ICT.

Website: http://www.cto.int/

Email: info@cto.int

European Network and Information Security Agency (ENISA)

Where: Crete, Greece

Funding: European Union and third countries

Mission: ENISA is the European Union's cyber-security agency and centre of expertise. Its responsibilities include ensuring the smooth functioning of the Internal Market, and improving the daily lives of the citizens and business, using broadband, online banking, e-commerce and mobile phones. ENISA aims to achieve a high and effective level of Network and Information Security within the EU, to assist the European Commission, member states and businesses to respond to and prevent security problems, and to assist in the technical preparatory work for updating and developing Community legislation in the field of Network and Information Security.

Website: http://www.enisa.europa.eu/

European Commission

Where: Brussels, Belgium

Funding: EU member states

Mission: In 2010, the European Commission put forward a proposal for a Directive on attacks against information systems. Its main novelty is the criminalisation of the use, production and sale of tools to effect attacks against information systems. In line with the Internal Security Strategy, the Commission will be setting up a European Cyber-crime Centre by 2013.

The Commission has also stepped up dialogue with the private sector, which controls a large part of information infrastructures.

Websites: http://ec.europa.eu/dgs/home-affairs/ http://ec.europa.eu/dgs/information_society/index_en.htm

European Police Office (EUROPOL)

Where: The Hague, the Netherlands

Funding: EU member states

Mission: As the EU's law enforcement agency it is Europol's responsibility to assist member states in the fight against international crime. Europol deals with the forensics and investigation of online crimes and has produced a threat assessment on internet facilitated organised crime (iOCTA) to contribute to the strategic planning for a European cyber-crime centre in 2012. Europol encourages international strategic and operational partnerships with the private sector and academia, raising awareness and points of contact and supports the use of crowd sourcing to gather intelligence on cyber-crime from internet users.

Website: www.europol.europa.eu

Forum of Incident Response and Security Teams (FIRST)

Where: Morrisville, North Carolina, U.S. (Secretariat)

Funding: Member CERTs

Mission: The Forum of Incident Response and Security Teams (FIRST) brings together security and incident response teams, including special product security teams from the government, commercial and academic sectors.

Website: http://www.first.org/

Email: first-sec@first.org

G8 Subgroup on high-tech crime

Funding: G8 member states

Mission: The G8's Subgroup on High-Tech Crime was started to enhance the abilities of G8 countries to prevent, investigate and prosecute crimes involving computers, networked communications and other new technologies. Over time, that mission has expanded to include work with third countries on such topics as combating terrorist uses of the internet and protection of critical information infrastructures. Countries are represented in the subgroup by multi-disciplinary delegations that include cyber-crime investigators and prosecutors, and experts on legal systems, forensic analysis and international cooperation agreements.

Internet Corporation for Assigned Names and Numbers (ICANN)

Where: Marina del Rey, California, U.S.

Funding: Not-for-profit public-benefit corporation with participants from all over the world

Mission: The Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) advises the ICANN community and Board on matters relating to the security and integrity of the internet's naming and address allocation systems. This includes operational matters, administrative matters, and registration matters. SSAC engages in ongoing threat assessment and risk analysis of the internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

Website: http://www.icann.org/

International Multilateral Partnership Against Cyber Threats (IMPACT)

Where: Cyberjaya, Malaysia

Funding: Not-for-profit comprehensive global public-private partnership

Mission: IMPACT is the cyber-security executing arm of the United Nations' specialised agency - the International Telecommunication Union (ITU). As the world's first comprehensive alliance against cyber-threats, IMPACT brings together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyber-threats.

Website: http://www.impact-alliance.org/home/index.html

Email: contactus@impact-alliance.org

Interpol

Where: Lyons, France

Funding: EU member states

Mission: Interpol's mission is to connect law enforcement in all member states and provide them with means to share crucial information. Interpol assists countries in the event of a cyber-attack and helps identify emerging threats and responses.

Website: http://www.interpol.int/en

International Telecommunications Union (ITU)

Where: Geneva, Switzerland

Funding: UN member states, and over 700 private companies and leading academic institutions

Mission: The ITU is the UN agency for information and communication technologies (ICT). Its responsibilities include allocating global radio and satellite orbits, developing technical standards and ensuring that technologies interconnect and improve ICT worldwide. ITU supports efforts to protect ICTs from cyber-threats. The ITU has also set up the Global Cyber-Security Agenda (GCA), a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration

with and between all relevant partners and building on existing initiatives to avoid duplicating efforts.

Website: http://www.itu.int/en/Pages/default.aspx

Email: itumail@itu.int

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Where: Tallinn, Estonia

Funding: NATO member states

Mission: The NATO CCDCOE was established to enhance capability, cooperation and information sharing among NATO, its members and partners in cyber-defence through education, research and development, lessons learned and consultation. Its aim is to be the main source of expertise in the field of cooperative cyber-defence by accumulating and disseminating knowledge. Its main areas of research include the legal and policy fields, concepts and strategy, tactical environment and critical Information Infrastructure Protection. The centre also develops a wide range of products and services for NATO.

Website: http://www.ccdcoe.org/

Email: ccdcoe@ccdcoe.org

NATO Communication and Information Systems Services Agency (NCSA)

Where: SHAPE, Belgium

Funding: NATO member states

Mission: NCSA is a service provider to NATO and its national customers. Wherever NATO deploys on operations or exercises, NCSA is there, providing communication and information systems (CIS) services in support of the mission. NCSA is NATO's first line of defence against cyber-terrorism and encompasses NATO Information Assurance Technical Centre (NIATC) and NATO Computer Incident Response Capability (NCIRC). NCIRC provides NATO with a range of highly specialised computer services, including incident detection, response and recovery that help ensure the security of NATO CIS. These services are delivered across the whole of the NATO CIS landscape, encompassing both operational and peacetime locations.

Website: http://www.ncsa.nato.int/

Email: ncsapao@ncsa.nato.int

Organisation of American States (OAS)

Where: Washington D.C., USA

Funding: Its 35 member states

Mission: The Inter-American Cooperation Portal on Cyber-Crime and the Working Group are two of the major outcomes of the process of Meetings

of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) aimed at strengthening hemispheric cooperation in the investigation and prosecution of cyber-crimes.

Website: http://www.oas.org/en/

Organisation for Economic Co-operation and Development (OECD)

Where: Paris, France

Funding: Its 34 member states and partner organisations

Mission: The OECD promotes policies to improve the economic and social conditions of people around the world. It provides a forum for governments to seek solutions to issues including cyber-security. It aims to secure privacy and data protection and launched an anti-spam toolkit for actors to better orientate their policies towards protecting against spam.

Website: http://www.oecd.org/

Organisation for Security and Co-operation in Europe (OSCE)

Where: Vienna, Austria

Funding: Its 56 member states and partner organisations

Mission: The OSCE seeks to promote the rule of law, inter alia by training of judges, prosecutors, lawyers, police and correctional officers, as well as through projects on criminal justice reform and legislative review, seeking to bring domestic laws in line with OSCE commitments and other recognised international standards, including those related to cyber-security.

Website: http://www.osce.org/

Email: info@osce.org

United Nations Interregional Crime and Justice Research Institute (UNICRI)

Where: Turin, Italy

Funding: UN

Mission: UNICRI is a UN entity mandated to assist intergovernmental, governmental and non-governmental organisations in formulating and implementing improved policies in the field of crime prevention and criminal justice. It aims to share and apply knowledge to assist governments to prevent and deal with cyber-crime.

Website: http://www.unicri.it/

Email: information@unicri.it

Glossary of companies

Accenture is the largest management consulting company in the world. Accenture Cyber Security Solutions offers cross-functional cyber-security programmes to secure vital IT-infrastructure.

BAE Systems is a British multinational defence, security and aerospace company headquartered in London. It is among the world's largest military contractors, and has extensive experience in the research and development of innovative computer network operations technologies.

BP is the third largest energy company in the world and is involved in oil, gas, petrochemicals, power generation and renewable energy.

Curesec is an IT security consulting company based in Berlin, Germany.

Deloitte Touche Tohmatsu is one of the largest accountancy and professional services company in the world. Deloitte's Global Public Sector group is also working in the field of cyber-security.

DEVOTEAM is an international information and communication technology consulting company headquartered in Brussels.

Hathaway Global Strategies is an independent security consulting company.

ING is a global financial institution involved in retail and investment banking and insurance services. It is therefore exposed to cyber-attacks and runs a big IT-security division.

Kaspersky Lab is a Russian computer security company. In addition to consumer products, Kaspersky Lab offers security applications designed for small business corporations and large enterprises.

Lexsi innovative security is an international information security consultancy company specialised in protecting information assets, strongly driven towards innovation and headquarted in France.

McAfee is a computer security company headquartered in Santa Clara, USA. It markets software and services to home users, businesses and the public sector.

NTT Communications is a subsidiary of Nippon Telegraph and Telephone (NTT) Corporation, one of the largest telecommunications companies in the world.

PwC is one of the world's largest professional services firms. Within its forensic services, PWC also works with clients to develop creative approaches to complex cyber-related matters.

Resolute Consulting is an American consulting company.

Security Europe is an information service specialised in EU civil security issues. As such, it also reports on developments in the EU cyber governance.

Genos Consulting is a Romanian information security consultancy firm.

Steptoe & Johnson is an international law firm. Cyber-security is one of its focus areas.

Stratsec, a subsidiary of BAE Systems, is an information security consultancy company based in Australia and South East Asia.

The SecDev Group is a Canadian company that provides consultancy services and conducts not-for-profit research in global security and violence. It equally undertakes research and consultancy on cyber-security.

Zurich is a financial services company focused primarily on insurance, also offering services in IT-security.

About the SDA

The SDA this year celebrates its 10th anniversary as the leading Brussels-based think-tank on security and defence issues. The SDA remains the only forum to bring together top representatives from across nations, institutions and sectors to discuss pressing global challenges, reaching both public and private sector decision-makers to make a real difference.

SDA Co-Presidents

Jaap de Hoop Scheffer
former Secretary General of NATO

Javier Solana
former EU High Representative for Common Foreign and Security Policy

"If current trends in the decline of European defence capabilities are not halted and reversed, many US policymakers may not consider the return on America's investment in NATO worth the cost."

Robert Gates, then US Defense Secretary
10 June 2011

"We must be careful not to allow the capability gap to become the credibility gap"

Anders Fogh Ramussen, NATO Secretary General
21 June 2010

The SDA raises awareness and anticipates the political agenda through international conferences, roundtables, evening debates, policymakers' dinners, studies and discussion papers. Visit www.securitydefenceagenda.org to download our publications and find out more about our activities.

Cyber-security initiative

As cyber-attacks continue to make daily headlines, the SDA has launched an ambitious cyber-security initiative. Encompassing reports, debates, and a strong online presence, this programme aims to bring coherence to the global cyber-debate, to separate fact from hype and make sense of the myriad actors in the field. The initiative ensures that all key stakeholders are heard in a balanced discussion, and that output reaches the key decision-makers.

"This is a battle we may not win. We need to act and to protect as quickly as possible"

Cecilia Malmström, European Home Affairs Commissioner
9 November 2011

"Cyber has redefined the front lines of national security. Just as our air and missile defences are linked, so too do our cyber defence networks need to be."

William J. Lynn, III, then US Deputy Secretary of Defense
15 September 2010

Visit the cyber-security website at www.securitydefenceagenda.org for the rest of the year's programme, video interviews, background documents, and SDA reports on cyber-security.

Security jam

The SDA constantly innovates to push the debate further. In 2010, it organised the first ever global security brainstorming, the Security Jam, which brought together over 4,000 people from 124 countries for a 5-day discussion. The report was presented to NATO Secretary General **Anders Fogh Rasmussen**, **Madeleine Albright** and her group of experts working on NATO's Strategic Concept, and **Felipe Gonzalez** and his group of European wisemen.

On March 19-23 2012, the SDA and IBM will partner with NATO ACT, the European External Action Service, the European Commission, EUCOM and the US Mission to NATO to bring together thousands of global security stakeholders. Representatives of national governments and armed forces, international institutions, NGOs, think-tanks, industry and the media will use this unique opportunity to collectively define the solutions to pressing security issues. The most innovative recommendations will be presented to the NATO and EU leaderships ahead of the May 2012 Chicago summits.

Log on to www.securityjam.org to register for this unique event.

VIP Jammers in 2010 included

Adm. James Stavridis, *Supreme Allied Commander Europe, NATO*

Alain Hubert, *Explorer, International Polar Foundation*

Josette Sheeran, *Executive Director of the World Food Programme*

Anne-Marie Slaughter, *Former Director of Policy Planning, US Department of State*

Gen. Stéphane Abrial, *Supreme Allied Commander Transformation, NATO*

Carl Bildt, *Minister for Foreign Affairs of Sweden*

A Security & Defence Agenda report

Author: Brigid Grauman
Publisher: Geert Cami
Date of publication: February 2012

The views expressed in this report are the personal opinions of individuals and do not necessarily represent the views of the Security & Defence Agenda, its members or partners.

Reproduction of this report, in whole or in part, is permitted providing that full attribution is made to the author, the Security & Defence Agenda and to the source(s) in question, and provided that any such reproduction, whether in full or in part, is not sold unless incorporated in other works.

SECURITY & DEFENCE AGENDA
Bibliothèque Solvay, Parc Léopold,
137 rue Belliard, B-1040, Brussels, Belgium
T: +32 (0)2 737 91 48 **F:** +32 (0)2 736 32 16
E: info@securitydefenceagenda.org **W:** www.securitydefenceagenda.org