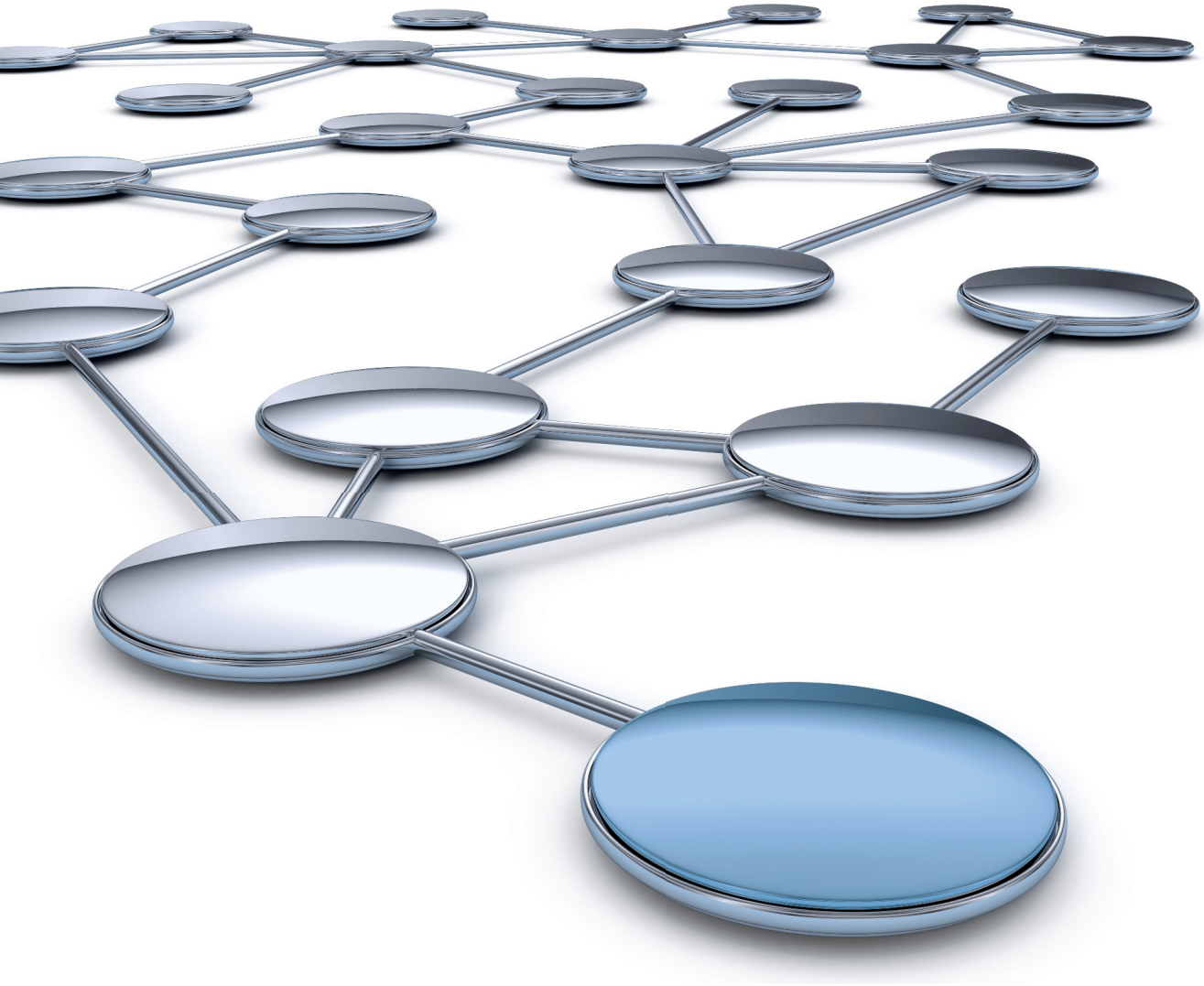

OSINT

Report 4/2010

ISN ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Authors: Florian Schaurer, Jan Störger

International Relations and Security Network (ISN)
ETH Zurich
Leonhardshalde 21, LEH
8092 Zurich
Switzerland
Tel.: +41 (0)44 632 04 24

osint@sipo.gess.ethz.ch
www.isn.ethz.ch

Project supervision: Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

OSINT Report 4/2010

Behind Walls or Out in the Open?

The Challenges of Protecting and Sharing Information

This report examines the prevalent classification and safeguarding procedures for sensitive national security information. It provides a synopsis of definitions, and casts light on the complex interplay between officially required secrecy and publicly desired transparency. The report furthermore addresses the implications of overclassification on the one hand, and authorized or unauthorized disclosures ('leaks') of classified information on the other, raising awareness for a more balanced governmental information security and sharing.

Information Security

The core principles of information security have long been understood to be *confidentiality, integrity* and *availability* (also known as the 'CIA Triad') which, meanwhile, have been augmented with three additional elements, namely *possession, authenticity* and *utility* (known as the 'Parkerian Hexad').

These components, explicitly or implicitly, establish a common ground of most corresponding legislation such as the Swiss 'Informationsschutzverordnung' (ISchV), the German 'Verschlusssachenanweisung' (VSA) or US Executive Order (EO) 13526 'Classified National Security Information'.

Every lack of information security affects at least one of the six principles of information security (except 'utility' which is mainly a qualitative benchmark), therefore any actionable sensitive information sharing regime needs to address all of them sufficiently.

Information security requires adequate and deliberate policies, instruments and procedures in order to be put into practical use. Any feasible implementation of protective measures will therefore, as a first step, need to take into account the underlying rationales and various forms of secrecy.

The Parkerian Hexad

1. Confidentiality means 'ensuring that information is accessible only to those authorized to have access'. It is supposed to prevent the unauthorized disclosure of information by limiting its legitimate audience.

2. Integrity means 'safeguarding the accuracy and completeness of information and processing methods'. It represents the trustworthiness and consistency of information and requires it not to be undetectably modifiable or corruptible.

3. Availability means 'ensuring that authorized users have access to information and associated assets when required'. It comprises the timely and reliable access to information by holders of the appropriate security clearance.

4. Possession means the legal ownership and physical control of information.

5. Authenticity means the undisputed credibility and traceability of both the information and the parties that have access to it. It is necessary to validate the veracity of the origin and authorship of information.

6. Utility means the usefulness or quality of information being of practical use for specific purposes, namely to best address the respective intelligence requirement.

(ISO/IEC 27000, 27001, 27002)

NOTES

Self-Regulated Secrets

Embarrassment secrets. 'The keeper of a secret motivated by embarrassment is motivated by the fear of 'what people will think' (or 'do') if the secret is revealed. [...] Oddly enough, experience shows us that embarrassment often leads the keeper of the secret to cause himself additional harm in attempting to avoid the revelation of a secret.'

Control secrets. 'In this case, the information being kept secret is believed by the keeper to relate directly to the control of assets, processes, or knowledge that might give others the ability to more directly do harm or gain advantage. [...] The estimation of harm that drives the valuation of a control secret may be inaccurate, but it is usually based in tangible factors.'

Privacy secrets. 'Privacy, for the purposes of this discussion, is the keeping of secrets out of a belief that others simply have no need or right to know.'

Externally Regulated Secrets

Legal secrets. 'The most obvious instance of external regulation of secrets is law or policy. [...] It is entirely possible for the keeper of the secrets to find that the regulations covering the handling of a particular secret may be derived from multiple regulating regimes that are not mutually, or even internally, consistent.'

Social cohesion secrets. 'Social cohesion secrets are those whose existence is not necessarily predicated on the inherent value of the secret, or the potential harm if it is revealed. Instead, these secrets are kept more for their usefulness in delineating 'us' and 'them'. [...] The actual objective content of the secret may be of little value, either to those holding the secret, or to any outsider. If such a secret is lost, it may easily be replaced - the value is not in the secret itself.'

Tradition secrets. 'This is the case where a secret continues to be kept beyond its useful life. [...] Whatever the reason, the basic characteristic is that the secret does not need to be kept any longer, but the processes, habits or regulations that governed the keeping of the secret continue on. Bureaucracies are especially suited to this type of secret, due to the lack of a mechanism for periodic review and revision of the regulatory and cultural structures that maintain the secret, either formally or by convention. Note that it may not even be intentional for such secrets to endure.'

(NSA Cryptologic Quarterly Spring/ Summer 2001)

Motivations for Secrecy

Pursuant to an engineer of the US National Security Agency (NSA), two groups and six types of secrets can be distinguished from each other (see above), proposing a viable taxonomy which illuminates the motivations of keeping (or not keeping), classifying and protecting alleged secrets.

Self-regulated secrets, being one major group, describe secrets which are held by their keepers themselves, whereas *externally regulated secrets*, being the other main category, point to secrecy that is regulated and dictated by someone other than the keeper or handler, such as a special classification authority or the governing body of an organization.

With reference to the valuation of secrets, a secret can either be of 'real' or illusory value or simply be irrelevant, meaning without utility. Concerning the derivation of secrets, the NSA article suggests to distinguish discretionary and mandatory secrets. With regards to the nature of secrets, factual, perceptual and attribution secrets are introduced. It is this complexity and multiplicity of what constitutes a secret that makes the current classification and clearance regimes often tilt at windmills and unamenable to formal automatisation, open to interpretation and vulnerable to poor execution. Additionally, all too often information security procedures (that is, classification and clearance) have not changed as quickly as the world and technology around, and those very motivational elements beneath, them.

NOTES

Classification and Clearance

Classification, which closely relates to confidentiality as elaborated above, describes the process and the resulting status of assigning a specified audience to sensitive information, the unauthorized disclosure of which would noticeably compromise national security. It is the attempt to legally restrict and control the accessibility of information by withholding it from general circulation.

While classification is an evaluation of the sensitivity of information itself, clearance or vetting requires a thorough evaluation of the trustworthiness of potential authorized individuals. Classification ultimately represents a material protection mechanism (relating to the worthiness for the protection of information), whereas clearance describes a personal protection mechanism (relating to the trustworthiness of the handler of information). Although they allude to separate operational and organizational layers, they remain naturally dependent.

In combination, classification and clearance assure that information can only be accessed by those who are assumed to not compromise it and who have a proven requirement to handle it. As classification and clearance must thus correspond to each other, they are usually grouped in three-to-four categories of access, e.g. the US categories TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C) (see EO 13526). Although unclassified information technically is not considered a fourth classification category, it is explicitly marked as UNCLASSIFIED (U). Both, the process of classification and the assignment of clearances are based on the damage that a disclosure of information would cause to national security as the sole criterion.

US President Obama recently improved the regulation on "Controlled Unclassified Information" (CUI) that requires safeguarding or dissemination controls for reasons other than protecting national security, such as privacy, security, proprietary business interests and law enforcement investigations. With his respective executive order he restricts and standardizes the use of CUI markings which have led to the creation of pseudo-secrets in the past.

In addition, Obama recently ordered classification to be explicitly justified and information to be rather classified lower in case of doubt. Yet, classification remains arbitrary – even if the danger of an unauthorized disclosure is well estimated and documented – when there is a lack of specific and consistent criteria to measure the severity of expected damage to national security. However, both US and German legislation provides little or nothing, at least not in unclassified form, to further define the different levels of damage to national security that would justify a respective classification and its implementation. In contrast, Switzerland is more specific about assumed damages to national interest, such as a derogation of Swiss economic interests which requires such information to be tagged at least as CONFIDENTIAL ('Vertraulich') or a possible derogation of Swiss intelligence's safeguarding of its sources and means which demands a classification as SECRET ('Geheim').

Need To Know

Besides clearance, the so-called 'need to know' (NTK), which gives individuals access to information of their clearance only if they need it to do their work is an additional internationally common safeguarding measure. It is linked to the security engineering concept of security through obscurity (STO), which arguably assumes that not knowing at all amounts to not being a potential threat to confidentiality.

An NTK is also what justifies access to compartmented control systems (CCS) above and beyond regular classification, such as, to take the US example, sensitive compartmented information (SCI), special access programs (SAP) and restricted data (RD). These are often confused with regular classification levels, of which RD only applies to sensitive information about special nuclear materials in accordance with the Atomic Energy Act of 1954.

However, in practice, an NTK is determined by principals, as the 'owners' of information rather than by the prospective recipients, with a mission need, an inherently inefficient approach which largely prevents serendipity and does not guarantee that the principal provides the handler with what he really needs to know. Recent US legislation is expected to shift the focus to the needs of recipients though. This may be a foundation for more efficient NTK procedures in the future, but it remains unclear how exactly this will be implemented. In theory, a possible two-fold NTK assignment could be an

NOTES

approach where the classification authority would combine its dissemination decision with IC-wide thematic tagging (regions, groups, etc.) of the information itself so that each holder of the appropriate clearance and with a mission-justified NTK for all information with certain tags would automatically have access, too. The challenge here is to develop a consistent taxonomy that is not too complex but still precise enough to respect the originally desired effect of the NTK-principle, which is to limit access to classified information as much as possible while sharing it with as many as necessary. Such an organizing principle requires the active contribution of lower echelons while they could still be supervised by the classification authority.

Protection and Sharing

The ultimate challenge for ICs remains the provision of a maximum of national, and increasingly also international, security. While nations will hardly give up the protection of their own existence and welfare as their primary goal, global security becomes increasingly relevant for national interests since nations are becoming more and more interdependent. Economic crises, natural disasters and armed conflicts are no longer affecting just their immediate regions of origin but also the world's welfare, freedom and safety. In addition, economic, ecological and militant developments are increasingly generating uncertainty and are thus gaining relevance for national security which evidently requires an enhanced international cooperation.

Today's mutual dependencies even between conflicting countries certainly contribute much to international security. Nevertheless, rationality is not equally spread among governments or insurgents world-wide, and with some parties cooperative equilibria may never work until they are finally defeated.

Given the absolute necessity for enhanced international cooperation and the indisputable existence of uncooperative, often hidden, players, an accurate identification friend or foe is key. With the loss of symmetry in security conditions, an easy confusion of friend and enemy and an increasing uncertainty over rather abstract threats, the overall need for security is omnipresent even among those who live in relatively high security. Particularly democratic and open societies are facing a frustrating dilemma between freedom and security, where the former may often be seen as a sacrifice for the latter. With the people having a claim and need for both and not being willing to abandon either, ensuring both is a continuous challenge to governments and can be done best in cooperation with allies, where important aspects of freedom, such as transparency, trust and exchange can be jointly practiced and actually form the foundation of a collective security facing common threats.

As shown, effective protection and sharing of sensitive information does presume an accurate and continuous assessment of the sensitivity of the information itself and of who is cooperative, given the sensitivity of information and a common interest in security. Sharing more information within national security enterprises and among allies seems questionable in times of weekly media reports of sensitive information that has been leaked, often by authorized individuals. This emphasizes the importance of an effective safeguarding system but can by no means be an argument against an equally effective intelligence sharing environment because both are in the interest of national security.

Intelligence exchange on national and international levels is nothing new, but it is, as discussed above, of increasing importance and has attracted new interest within ICs world-wide, especially since a lack of information sharing was found to have contributed to intelligence failures that led to the inability to prevent 9/11. In fact, there are long-established bilateral and even multilateral exchanges between intelligence services of different countries. One could speak of an information trade where the price of a specific information is determined by the value it has for the receiving and providing services. Through bargaining, partners come to terms of an efficient trade. However, this presumes mutual proofs of confidence and transparency about the true quality of the traded information. For this, a common quality rating system is necessary to ensure the comparability of analytical reasoning and its ultimate value for addressing the respective intelligence requirement.

This is why intelligence sharing, be it on a national level or between different countries, requires a nationally consistent and internationally compatible classification and marking system. While the US has initiated

NOTES

official programs to foster intelligence sharing and cooperation, such initiatives have failed so far elsewhere. Official projects for internal information sharing supported by new technologies and media such as 'Intellipedia' of the US Intelligence Community and 'Diplopedia' of the US State Department are still exemplary.

Standardization and Compatibility

Especially in the case of a Gordian intelligence apparatus as in the US, a nationally consistent and internationally compatible classification and marking system is essential for a balanced protection and sharing environment. In January 2008 the US Office of the Director of National Intelligence (ODNI) published a report on the findings and recommendations on intelligence community classification guidance which reveals a lacking transparency of 'the reasons for setting classification and limited guidance for discriminating between classification levels. Most of the guides were agency- or program-specific. In situations where users perceived conflicting guidance, they found it difficult to discern which classification guide or level should take precedence, leading to over-classification in many cases'. It remains questionable whether the President's order to loosen classification in cases of doubt to avoid overclassification will be effective in practice, given uncertainty about the correct procedures, especially if agents risk being held responsible for under-classification or leaks.

Providing standards and incentives for an appropriate classification are key to both protecting and sharing intelligence. Better understanding the motivation for overclassification can help to develop respective system reforms. In the US, new principles such as classifying as low as possible and as high as necessary, the improved use of unclassified controlled information (CUI) and the imperative to not classify information to hide inefficiencies or illegal actions are important steps into the right direction but will have to prove workable. Illegal actions or inefficiencies of the government can cause political tensions or even unrest and thus potentially damage national security. As long as 'national security' remains largely undefined, yet the ICs ultimate mission, the prevention of political upheaval could be given priority in such a case, despite its problematic legal and moral implications.

Authorized Disclosure

An efficient and appropriate classification system must also regulate under what circumstances information can be reclassified or declassified. In democracies, government transparency is vital to its credibility and support among voters. This requires a government to keep the public informed about its actions unless there are higher reasons which legally justify secrecy. Information will be outdated at some point, and therefore be automatically declassified following legal retention periods in most cases. Likewise, it may be overclassified due to the aforementioned reasons and thus qualify for manual review and declassification. The more information is overclassified, the less it can be shared with intelligence partners or with the public.

Declassifying information can be based on a variety of motivations. For example, there may be the necessity to warn the public of an immediate threat to national security where the interest in national security and transparency are not in conflict. This must however be done with great care due to the implied danger of causing mass hysteria and panic. Furthermore, adversarial forces must be assumed to have access to the same public information and will use it in their favor. Taliban fighters in Afghanistan are for example believed to have improved their tactics after reading unclassified ISAF field manuals.

Recent public announcements concerning an imminent terror threat in Germany triggered a discussion about what the public should be told in such cases. Even an open society cannot afford too much security-relevant information to be released because it will make its defense predictable for an enemy who puts much effort into being unpredictable. Knowing this, public releases can also be used to provoke a reaction of an unidentified enemy who might then be revealed. It must not be underestimated how easily conspiracy theories develop after public announcements of an imminent threat; is this just to find voters' support for more defense spending and increased security measures? The consequences of sharing information, especially with the public, can be intricate and dangerous and must therefore be anticipated carefully case by case before considering authorized disclosure, such as under the US Freedom of Information Act (FOIA).

NOTES

Unauthorized Disclosure

Almost four decades after Daniel Ellsberg leaked the 'Pentagon Papers' which - according to US President Nixon's Solicitor General - were massively overclassified and de facto posed no significant threat to national security, the unwarranted proliferation of sensitive information has reached new speed and scale with ubiquitous channels of assumed anonymous data transport readily at hand for virtually everyone. Thus, it is only logical that a technically relatively simple whistleblowing platform like WikiLeaks (being something like a web-based 'dead-letter-box') repeatedly succeeds in exasperating advocates of government secrecy, while teaming up with the media to hype yet another 'largest leak in history' and enjoying a rather uncritical but noticeable public and moral acclaim. The irony of fate has it that even the US Army Counterintelligence Center's strategy on how to crack down on WikiLeaks was leaked to and published by the organization itself.

In the US alone, some 850,000 individuals are granted top secret clearance according to The Washington Post's latest investigation into 'Top Secret America'. Many millions more do have a secret clearance, raising the question how secret a government's secrets really are. As US Supreme Court Justice Potter Stewart put it, if everything is secret, nothing is. It comes as no surprise that when James Clapper took over as Director of National Intelligence (DNI) in August, he sent an internal memo to all 16 US intelligence agencies reminding them to not tolerate the compromise of information security. The memo was leaked to the media several hours later.

Since nowadays it is possible to securely share classified information in a timely manner over long distances (that is providing for its integrity and authenticity through the use of encrypted networks such as the US SIPRNet and JWICS or the German JASMIN and SINA), most leaks are not the result of illegal interception of communications from the outside, but of flawed security procedures (accidentally) and insufficient confidentiality on the inside (intentionally). Whereas the first mainly relates to the external regulation of secrets, the latter relates to the internal regulation of secrets and an individual's intrinsic motivation for not keeping them. Motivation to breach confidentiality can be found in many places, including selfish calculation, for example, selling confidential bank account information to foreign authorities, which caused this year's disputes between the governments of Switzerland and Liechtenstein on the one side and Germany on the other side.

Interestingly, an official UK government response from March 2010 acknowledges that 'there are exceptional circumstances in which a civil servant could be justified in leaking material in order to expose serious wrongdoing. This would need to have followed a failure of proper channels both of disclosure and challenge within government. In short, it must be a last resort'.

This concession indicates that the primary reason for leaking is not the mere access to information but the lack of 'accessible, effective and visible channels by which civil servants of all grades can raise genuine concerns about the conduct of government', as a House of Commons report from 2009 states, only taking into account an employee's discontent and frustration, yet hardly his or her personal greed or craving for recognition.

As not only recent history shows, it is becoming ever more complicated to successfully and permanently safeguard classified information and to sustain confidentiality of and physical control over it. Mere claims of legal possession and punishability have proved insufficient to restore that power and to make secrecy oaths work once and for all. At the same time, legal hierarchy and organizational practice such as overclassification and understandardization hinder sensitive information from being readily available for those who eventually may tip the scales.

While many legal scholars argue that the dissemination of classified information in an unclassified format, such as a newspaper, also constitutes a form of unauthorized disclosure (namely a secondary or derivative leak), exponents of the freedom of press counter that the press itself cannot be held responsible for the original and clearly litigable leak. Accordingly, secondary leaks of classified material by the press have, potentially instrumentalized by politics, so far rarely been prosecuted as crimes; a growing necessity for legal regulation is evident.

NOTES

Consequences of Recent Leaks

The impact of WikiLeaks is as much discussed as its prosecution. Both public and government interests are not always in line with national security or freedom of information. While governments are under pressure and are desperately seeking effective countermeasures, the public, depending on its interest in the information, is rather unsure whether Julian Assange, who was imprisoned temporarily due to unrelated accusations, or even the alleged original leakers must be considered heroic activists or simply criminals. Events will have to be examined more closely, given the diversity and sensitivity of leaked information and the potential legitimacy of public interest.

This December, the US Congressional Research Service (CRS) concludes in a report that a prosecution of WikiLeaks would be legally and politically challenging because there is no known precedent 'in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it'. The US Espionage Act currently applies to information related to national defense only, thus excluding a majority of the recently leaked diplomatic cables. Furthermore, the question of whether the publication of unlawfully acquired information must be protected by the First Amendment, guaranteeing the freedom of press, remains unanswered, although the US Supreme Court has decided in favor of the First Amendment in preceding cases. While publishers may remain protected, the directly affected parties are currently attempting to make quick work of the alleged original leakers who usually hold a proper and legally binding clearance.

This December, the White House announced several mitigation initiatives, including policy and practices reviews, as well as immediate safeguarding measures in response to the recent 'unlawful and irresponsible' disclosures of classified information on WikiLeaks.

'The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. During the past decade, departments and agencies have tried to eliminate those gaps, resulting in considerable improvement in information-sharing. At the same time, federal policies underscore the importance of the existing prohibitions, restrictions, and requirements regarding the safeguarding of classified information.'

The President's Intelligence Advisory Board (PIAB) will examine 'the balance between the need to share information and the need to protect information'. The Office of Management and Budget (OMB) has directed each department or agency that all reviews 'should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure that users do not have broader access than is necessary to do their jobs effectively, as well as implementation of restrictions on usage of, and removable media capabilities from, classified government computer networks.'

Besides those inter-agency efforts, individual US departments and agencies are taking additional measures such as the deployment of an automated system backed by specially trained staff who monitor users and networks for suspicious activity not readily apparent. A proposal for such a program called Cyber Insider Threat (CINDER) has been made at DARPA recently with the goal of detecting and responding more quickly to insider threats. Along with the introduction of regular intensified information assurance trainings that focus on awareness of activity associated with insider threats for all employees handling classified information and immediate safeguarding measures, there will also be random physical inspections by teams consisting of counterintelligence (CI), security, and information assurance (IA) experts. Immediate safeguarding measures include suspending access to the Department of State's (DoS) Net-Centric Diplomacy (NCD) diplomatic reporting database, restricting access to the DoS classified web (ClassNet) and SharePoint content to users of the highly secure Joint Worldwide Intelligence Communications System (JWICS) cleared up to TOP SECRET while suspending access to the aforementioned content over the medium-security network SIPRNet cleared up to SECRET only.

Striking the Balance

Moving forward from an anxious information protectionism (with its focus on confidentiality) and all too idealistic sharing initiatives (with its focus on availability) to a versatile, well-balanced and responsive governmental information security doctrine will be a challenge. This means moving the information itself towards center-stage and not just the people involved in handling it. In other words: evaluating, case by case, the substance and relevance of information

NOTES

must be the first step in determining how and by whom it shall be processed. The processing requirements should then steer and justify the access restrictions, and not vice-versa.

The more thoroughly clearance and vetting procedures are conducted (to ensure confidentiality and trust) and the more the matter-of-fact relevance of information itself determines to what degree it needs to be safeguarded (to ensure utility and significance), the less arbitrarily information can be classified and the less self-serving an altogether unavoidable secrecy will be. At this point, one ought not confuse the necessity for an open flow of information within an organization with the public desire for transparency and freedom of information. Just enhancing secrecy and re-inventing its semantics does not equal enhancing security, but damages it, within and outside of the intelligence apparatus. There is a deluge of irrelevant and undigested secrets that can neither be processed nor protected.

Information security does not enforce itself; classification without adequate protection is a paper tiger. Yet, protecting what is not genuinely confidential is dangerous, as it consumes the very resources necessary to spot the subtle and tenuous unknowns of collection and analysis. At the same time, unauthorized disclosures will ultimately undermine the legitimate quest for truth, transparency and trust because governments will react with more sealing-off.

NOTES

Sources and Links

Bundesministerium des Innern (BMI): Verwaltungsvorschrift zur VSA
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/VSA.html

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS): Klassifizierung / Behandlung klassifizierter Informationen
http://www.vbs.admin.ch/internet/vbs/de/home/themen/sicherheit/informationsschutz/klassifizierung.html

Jennifer K. Elsea, Congressional Research Service (CRS): Criminal Prohibitions on the Publication of Classified Defense Information
http://www.fas.org/sgp/crs/secrecy/R41404.pdf

Federation of American Scientists (FAS): Secrecy and Security Library
http://www.fas.org/sgp/library/index.html

Iternational Organization for Standardization (ISO): ISO/IEC 27000, 27001, 27002
http://iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on

National Security Agency (NSA): Toward a Taxonomy of Secrets
http://www.nsa.gov/public_info/_files/cryptologic_quarterly/toward_a_taxonomy.pdf

Office of the Director of National Intelligence (ODNI), United States of America: Intelligence Community Classification Guidance Findings and Recommendations Report
http://www.fas.org/sgp/othergov/intel/class.pdf

Prem Mahadevan: Intelligence Agencies - Adapting to New Threats
http://www.sta.ethz.ch/CSS-Analysis-in-Security-Policy/No.-82-Intelligence-Agencies-Adapting-to-New-Threats-October-2010

Schweizerischer Bundesrat: Verordnung über den Schutz von Informationen des Bundes
http://www.admin.ch/ch/d/sr/510_411/index.html

The President of the Unites States: Executive Order 13526 - Classified National Security Information
http://www.archives.gov/federal-register/executive-orders/2009-obama.html#13526

The President of the Unites States: Implementation of the Executive Order - Classified National Security Information
http://www.whitehouse.gov/the-press-office/presidential-memorandum-implementation-executive-order-classified-national-security

The President of the Unites States: Executive Order 13549 - Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities
http://www.archives.gov/federal-register/executive-orders/2010.html#13549

The President of the Unites States: Executive Order 13556 - Controlled Unclassified Information
http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information

The President of the Unites States: H.R. 553 - The Reducing Over-Classification Act
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h553enr.txt.pdf

The Washington Post: Top Secret America
http://projects.washingtonpost.com/top-secret-america/

UK Commons Select Committee: Leaks and Whistleblowing in Whitehall
http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-administration-select-committee/inquiries/former-inquiries/leaks-and-whistleblowing-in-whitehall/

US Government: Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information
http://www.whitehouse.gov/the-press-office/2010/12/01/fact-sheet-us-government-mitigation-efforts-light-recent-unlawful-disclo

United States of America: Atomic Energy Act of 1954
http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf#pagemode=bookmarks&page=14

NOTES

ISN
ETH Zurich

INTERNATIONAL RELATIONS AND SECURITY NETWORK

ETH Zurich | Leonhardshalde 21, LEH | 8092 Zurich | Switzerland
Tel: +41 (0)44 632 04 24 | Fax: +41 (0)44 632 14 13
www.isn.ethz.ch | osint@sipo.gess.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich