Defining the Scope of National Security: Issues Paper for the Open Society Justice Initiative National Security Principles Project[1]

Toby Mendel
Executive Director
Centre for Law and Democracy
May 2011

Introduction

The Open Society Justice Initiative is currently engaged in a process of developing a set of Principles on National Security and the Right to Information (Principles). This paper is intended as a contribution to that process. Specifically, it addresses the issue of how to define the scope of national security in the context of the Principles.

References in this paper to the Principles are references to the 2 May 2011 draft. The draft includes two main principles which define the scope of national security. Principle 2 defines the core characteristics of national security, while Principle 11 provides a list of the specific categories of information to which restrictions may be applied on the basis of national security. This is a good approach, as it allows for more detailed elaboration of the content of national security through the Principle 11 list, but subjects this list to the overall definition of national security provided in Principle 2.

The paper is in two parts. The first part discusses a number of different issues which are relevant to the definition of national security. The second part proposes concrete language for Principles 2 and 11, based on the 2 May 2011 draft. In both cases, the paper assumes that the purpose of defining national security is to understand the corresponding scope of (legitimate) restrictions on the right to

[1] This paper has been developed as part of the process being overseen by the Open Society Justice Initiative to develop a set of principles on national security and access to information. It is thus tailored to addressing some of the key outstanding issues that have arisen through that process. The Centre for Law and Democracy would like to thank the Open Society Foundations for their support for this work. We also note that the paper will be made available shortly on OSJI's website focusing on access to information issues, http://www.right2info.org/.

information. The term right to information, as used in this paper, refers to rules both limiting individuals' access to information held by public authorities and providing for sanctions for officials and others who release information.

Issues

Purpose of Definition

Before attempting to define national security, we need to understand the purpose to be served by the definition. In the context of the Principles, there are two purposes: defining the scope of information to which access may be refused on national security grounds (or, conversely, to which access must be provided); and as a key element in defining the circumstances in which individuals may be punished for releasing information relating to national security (i.e. setting the parameters for disclosures which may attract such punishment). These two purposes may be understood as two sides of the right to information: the right to access information and the corresponding obligation on public authorities to disclose that information (and consequent protection for doing so).

The Principles clearly tie the first of these purposes (access) to the definition of national security as set out in Principle 11 (and by implication Principle 2); this is clear from the very name of Principle 11. The scope of prosecutions for disclosing information (the second purpose) is not, however, so clearly linked to Principle 11. Principle 39 allows prosecutions for the disclosure of information where this is, among other things, pursuant to a "narrowly drawn statute which clearly identifies the category of information" subject to protection.

It is not immediately clear that the same definition should apply in the context of these two different purposes. In practice, in many countries, there is a gap between at least some exceptions in access to information laws, which define what information public authorities are *not required to disclose*, and rules prohibiting disclosure of information, which define what information public authorities *must not disclose*. In other words, there is a margin of discretion left to officials regarding information which they are neither required to disclose nor prohibited from disclosing. On the other hand, in some countries, the rules are precisely aligned, for example by postulating exceptions to the right of access in a mandatory form, so that officials 'must refuse', rather than 'may refuse', requests for included information.[2]

In relation to national security, there are strong arguments for closely aligning these rules, including the need to protect civil servants from potentially serious sanctions for wrongly exercising their discretion. Furthermore, where exceptions to the right of access are very narrowly defined, this automatically narrows or eliminates the

[2] This is the case for many of the exceptions in the South African Promotion of Access to Information Act, No. 2 of 2000. Perhaps ironically, the national security exception in that Act, found at section 41, is discretionary rather than mandatory in nature.

scope of any discretion. If information may only be withheld where its disclosure really would pose a risk of harm to national security, the same information must be withheld, for it cannot lie within the discretion of officials to put national security at risk. This may be contrasted with some other limitations on the right to information, such as the one in favour of internal deliberations, where it is reasonable to grant some discretion to public authorities to decide whether or not to disclose the information.

It is therefore recommended that the rules on requirements to disclose and prohibitions on disclosure be aligned in the Principles. This means that Principle 39 should allow for punishment for disclosure of information only where that information falls within the scope both of national security as defined by Principle 2 and the specific categories listed in Principle 11.

Limitative Impact

It is not clear from the structure of the Principles to what extent the narrow definition of national security proposed will actually have the desired limitative impact in relation to both access and punishment in the context of national security information. This is because the narrow definition does not formally rule out the withholding of information or the application of punishment for information falling outside its scope, for the protection of interests other than national security. Thus, Principle 2(c) excludes mere economic impact from the definition of national security, but it does little to stop States rendering information secret on the basis of its economic impact, or even criminalising the disclosure of information deemed to be economically sensitive, for example on the argument that this is necessary to protect public order or the rights of others.[3]

Principle 14, listing categories of information of high public interest, helps in this regard by making it clear that certain types of information may never be rendered secret. But it does not comprehensively address the problem, because it is limited in scope to information of important public interest.

This is a difficult problem, because it is not possible to address within the scope of the Principles all of the categories of information that may not be withheld at all, or even those that States have tried to withhold abusively on national security grounds. And some information which should not be treated as sensitive on national security grounds may legitimately be withheld on other grounds. For example, certain types of economically sensitive information may be withheld under almost all access to information laws.[4]

[3] Both legitimate grounds for restricting freedom of expression under international law.

[4] To give just one example, Article 13 of the Mexican Federal Transparency and Access to Public Government Information Law, generally considered to be a progressive law, establishes an exception for information the disclosure of which would "harm the country's financial or economic stability". The law is available in English at: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf (and in the Spanish original at: http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf).

It is probably not possible to address this problem fully in the Principles but a partial solution may lie in noting that all exceptions to the right of access and any rules providing for punishment for the disclosure of information – which are both restrictions on freedom of expression under international law – may only be justified by reference to the established grounds for such restrictions (i.e. the rights or reputations of others, national security, public order, or public health or morals).[5]

Foreign Relations: Classification Coincidence or Substantive Link

The definition of national security in Principle 2(b) refers specifically to "the maintenance of foreign relations", but only to the extent that this is linked to the protection of national security, *per se*. It is obvious that foreign relations comprise far more than just national security, since they are also importantly related to economic matters, sports and culture, the environment and many other areas of interaction between States.

At the same time, an important part of foreign relations do relate to national security. It could be argued, however, that several other accepted grounds for secrecy, at least in access to information laws – such as commercial confidentiality, investigation of crime and internal deliberations – also overlap with national security in a similar fashion. For example, a private company may own the intellectual property rights to a sensitive weapons system, or a criminal investigation could relate to a terrorist threat. Certainly the degree of overlap with foreign relations is more extensive, but it is not clear this justifies a special mention of foreign relations within the main definition of national security.

Another consideration is that the systems for protecting secrets in some countries are the same for foreign relations and national security, whereas different systems are used to protect other sorts of confidential information. In particular, in these countries classification systems are used to protect national security and foreign relations secrets, and not to protect some other categories of confidential information.[6]

In the United States, for example, the President has the power to classify information as secret on the basis of national security or foreign relations, and this is reflected in the access to information law, which does not apply to information properly classified as secret in relation to these two categories pursuant to a presidential executive order.[7] However, this arguably flows from a particular constitutional arrangement, whereby the President exercises powers in relation to national security and foreign relations.[8]

---

[5] This list is drawn from Article 19(3) of the International Covenant on Civil and Political Rights, which sets out the test for restrictions on freedom of expression under international law.

[6] Thus, privacy may be covered by a data protection law and commercial confidentiality is may be protected through contractual arrangements.

[7] Freedom of Information Act, 5 U.S.C. §552(b)(1).

[8] Pursuant to Article II § 2 of the Constitution, the President is the commander-in-chief and has the power to conclude treaties (with the consent of the Senate). See Meredith Fuchs, *US Law on FOI and*

South Africa includes "defence, security and international relations" under the same exception to the Promotion of Access to Information Act.[9] On the other hand, the current draft of the South African Protection of Information Bill, which would criminalise certain types of disclosures, includes national security and foreign relations, but also commercially sensitive information and privacy, within the scope of the system of classification.[10] This is still being debated in South Africa. However, the main civil society platform campaigning for reform of the Bill, the Right2Know campaign, has demanded, among other things, that the law: "Limit secrecy to strictly defined national security matters and no more."[11]

In many countries, there is no special relationship between national security and foreign relations. In the United Kingdom, for example, the Official Secrets Act, 1989, variously covers information relating to "security and intelligence", "defence", "international relations" and "crimes and special investigations".[12] In Canada, the Security of Information Act establishes various offences by reference to the notion of a purpose which is "prejudicial to the safety or interest of the State", which is defined in section 3(1) to include a wide range of interests which go well beyond security interests, and include causing harm to the health and economic well-being of the people.[13]

In other countries, systems of secrecy and classification cover all types of confidential information. In Bulgaria, the Protection of Classified Information Act defines two types of secrets: State secrets and official secrets. The former includes national security, defence, foreign policy and protection of the constitutionally established order. The latter covers anything the disclosure of which would "influence unfavourably the interests of the state or would hamper other legally protected interests".[14]

In Mexico, classification applies to all information which may be withheld from the public pursuant to the access to information law, regardless of the grounds. The main independent oversight body, the Federal Institute of Access to Information and

---

Classification, draft on file with the author.

[9] See note 2. Even though it is included in the same clause, protection of foreign relations is treated somewhat differently under the South African law.

[10] Section 15. Available at: http://www.parliament.gov.za/live/commonrepository/Processed/20100512/206191_2.pdf. There are currently proposals to remove the reference to commercial information but this is still being debated by the parliamentary committee discussing this draft law.

[11] See their campaign statement, available at: http://www.r2k.org.za/component/content/article/37-resource/68-r2k-founding-statement.

[12] Sections 1-4. Different sets of rules apply depending on whether the individual is a member of the "security and intelligence services" or simply a "Crown servant or government contractor". The law is available at: http://www.legislation.gov.uk/ukpga/1989/6/contents.

[13] R.S.C., 1985, c. O-5, Available at: http://laws-lois.justice.gc.ca/eng/acts/O-5/FullText.html.

[14] Official Gazette No. 45/30.04.2002, Articles 25 and 26. Available at: http://www.aip-bg.org/library/laws/pcia.pdf.

Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos), sets rules regarding classification and may review classification.[15] As in the United States, it is only where documents are properly classified pursuant to the rules that access to them may be refused.

In some States, the rules focus more narrowly on security issues. Thus, in Estonia, the State Secrets Act does include information classified as secret by other States and inter-governmental organisations, but the vast majority of the provisions in its various rules on classification focus on national security in the strict sense of the word.[16]

We may thus conclude that there is no particular established practice in this area and that in most States classification procedures do not apply specifically to national security and foreign relations information. It is thus recommended that the reference to foreign relations be removed from Principle 2(b).

General Relevance of Classification Systems

Above, the issue is whether foreign relations should be included in the scope of the definition of national security. A different issue is raised by Principle 16, which calls for the separate *safeguarding* of classified national security information, on the one hand, and information which is being protected for other reasons, on the other.

It is perhaps useful to distinguish between two main approaches to classification. In many countries – including United States, Mexico and Slovenia[17] – classification, if correct according to the rules, serves to render information secret. An advantage of this approach is that it is clear and allows for procedural safeguards to be built into the system for classification. A disadvantage is that it can introduce rigidities into the system, and lead to information being withheld even though there is no persisting interest in secrecy.

In other countries – such as Canada and the United Kingdom – classification is simply an internal direction to civil servants and is not determinative with respect to either a request for the information or the question of whether or not an individual may be punished for disclosing it. In the United Kingdom, for example, the main test for applying sanctions under the Official Secrets Act is whether a disclosure is damaging, while it is a defence if the person did not know and had no reasonable cause to believe that the information fell into the relevant category or would be damaging.

In theory, this approach to classification should lead to decisions about openness

[15] Articles 15-17 of the law. See note 4.

[16] 1999. See sections 4[1] to 8. Avaiable at: http://www.legaltext.ee/en/andmebaas/ava.asp?m=022.

[17] The Classified Information Act. Official Gazette RS, No. 87/01, as amended. Available at: http://www.uvtp.gov.si/en/legislation_and_documents/legal_acts_in_force/.

being made on the merits of each case. In practice, however, it tends to be characterised by an absence of procedural protections, which results in over-classification. This, in turn, has a practical impact on decision-making regarding disclosure, even if legally it should not.

Formally, there should not be any particular relationship between the definition of national security and the various classification procedures and approaches adopted in different countries. But Principle 16 forges a link because in most countries there is a close relationship between classification and the safeguarding of information.[18]

It is clear from the analysis above that different States include different types of information their classification regimes. Principle 16 would require them to segregate national security information from the other types of information that they classify for purposes of safeguarding the information. It is not clear what the rationale behind this is, and it is recommended that this be reconsidered.

At the same time, the rest of the proposed rules on classification in the Principles are useful, as they aim to restrict the application of classification labels on the basis of national security to information which really is national security sensitive. This is important regardless of which primary approach to classification is employed in a given country.

Levels of Classification

In many countries, the law defines different levels of classification and allocates different categories of information to each level. Thus, the laws of Bulgaria, Estonia and South Africa (in that case the proposed Protection of Information Law), all define different lists of information for the different classification levels.

The Principles specifically decline to take a position on whether different levels of classification should be employed, but they do purport to reserve the highest level of classification for more serious risks of harm (see Principle 18). This can be justified on the basis that it is not for a statement of principles to delve into nuts and bolts questions regarding how information security systems should work.

On the other hand, there may be benefits to incorporating the idea of different levels of classification into the definition of national security. This would potentially allow for the list of categories in Principle 11 to be allocated to different classification levels, or for any additional categories to be restricted to certain levels of classification.

For example, a thorny issue is what level a risk must rise to for it to qualify as a national security threat, as opposed to merely criminal behaviour (see below). One potential way to address this is to correlate levels of risk with levels of classification. Thus, a risk that threatened the very life of the nation could qualify information (as

[18] Note that this is not always the case, for example in Canada and the United Kingdom.

needed) as top secret, while a risk that 'only' threatened significant damage could be limited to a lower level of classification. In the proposed South African law, for example, 'confidential' applies to disclosures which may be 'harmful' to security, 'secret' applies to those which may 'endanger' security and 'top secret' is reserved for those which may cause 'serious or irreparable harm'.[19]

An approach along these lines could help ensure that the most serious penalties were reserved for the most serious situations. However, it could also cut across the logic in many schemes which links level of classification to the degree of sensitivity of the type of information rather than the risk.[20] Another problem with this approach is that it is extremely difficult to define the level of risk with any degree of precision. The South African example above demonstrates this: the terms used – harmful, endanger security and serious harm – are all extremely vague and malleable.

Levels of Threatened Harm

The Principles properly exclude 'peripheral' issues such as the economy or other matters relating to general welfare from the scope of the definition of national security (see Principle 2(c)). Extending the definition of national security to include these sorts of considerations would substantially broaden the definition to include many matters that have only a tangential relationship with national security.

On the other hand, it may be more difficult to draw a clear line, at least in relation to risks of a violent nature, between localised situations which should be treated as ordinary criminal matters, and those which rise to the level of a national security threat. Thus, in Mexico today, the destabilisation caused by drug-related violence has reached a level which arguably poses a serious threat to the very stability of the nation and which should, as a result, be classified as a national security-type threat.

In many countries, the issue of 'policing' national security threats is addressed under the rubric of intelligence. The provision in United States Presidential Executive Order 13526 – Classified National Security Information is typical, referring to "intelligence activities (including covert action), intelligence sources or methods, or cryptology".

The problem with this is that intelligence is potentially an extremely broad term. For example, the South African Protection of Information Bill includes a detailed definition of intelligence that includes 'crime intelligence' (relating to the prosecution of apparently any crimes) and 'domestic intelligence' (which includes intelligence on activities that threaten the constitutional order, the safety or well-being of citizens or the preservation of all publicly-owned goods). The definition of intelligence in the access to information law is a bit narrower, but still covers the

[19] Similarly, in Slovenia the law defines the different levels of classification by reference to the seriousness of the threat to security. Note 17, Article 13.

[20] This is the case, for example, in Estonia. See note 16.

detection of 'hostile activities'.[21] Overall, there is little in the various provisions defining national security in different laws to limit the scope of the concept of intelligence.

The wider challenge here is to determine what conditions transform what would otherwise be an ordinary criminal or administration of justice issue into a threat to national security. This is complicated by the fact that threats to security can take the form of attacks on almost any national system. The attacks of 9/11 were directed at the Pentagon, a traditional military target, but also at the World Trade Center, a civilian target.

Rather than trying to create a list of national security targets, it probably makes more sense to try to identify a number of factors that together qualify an activity as involving national security. A potentially helpful idea comes from a 2004 Canadian government policy paper, *Securing an Open Society: Canada's National Security Policy*, which notes:

> The focus is on events and circumstances that generally require a **national response** as they are beyond the capacity of individuals, communities or provinces to address alone.[22] [emphasis added]

Another factor could be the need to employ the armed forces to address a situation (albeit linked to other elements of the definition, since the armed forces are commonly employed in natural disaster situations). A concern here is that some countries may be willing to use the armed forces in significantly lower-level security situations than other countries.

The purpose of any attacks or intended attacks, or the intent underlying them, could be another factor. Where these are of an 'ordinary' criminal nature, the activity would not fall under the rubric of national security, but where they were more security-related, they might.

In Israel, there are presently moves to amend the secrecy law to distinguish cases where the purpose of the leak was to spy on the State and cases where the leak posed a threat to national security but was not specifically aimed at spying.[23] Part of the definition of prejudicial purposes under the Canadian Security of Information Act includes crimes punishable by two or more years imprisonment, but only where these are committed to "advance a political, religious or ideological purpose, objective or cause or to benefit a foreign entity or terrorist group".[24] This refers to two distinct kinds of objectives, one defined by its motivation (political, religious or

[21] Section 41(2)(d)(ii).

[22] Page 3. Available at: http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf.

[23] The so-called Anat Kam law, named after a solider who leaked information to the press. See: http://www.israelnationalnews.com/News/News.aspx/142858.

[24] Note 13, section 3(1)(a).

ideological cause) and one by its intended beneficiary (foreign entities or terrorist groups).

The definition of terrorism has proven elusive under international law, but the special international mandates for the protection of freedom of expression have defined it in the context of restrictions on that right, as follows:

> The definition of terrorism, at least as it applies in the context of restrictions on freedom of expression, should be restricted to violent crimes that are designed to advance an ideological, religious, political or organised criminal cause and to influence public authorities by inflicting terror on the public.[25]

Many national definitions of defence or national security include a focus on threats from abroad. The Official Secrets Act, 1989, of the United Kingdom defines a disclosure as being damaging to defence if it undermines the capability of the armed forces, or "endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad". The first part of this definition reflects a fairly traditional understanding of defence, but the second part goes far beyond anything related to defence or security, to include almost any foreign interest of the United Kingdom.

There would appear to be little to justify a focus on foreign threats in a modern definition of national security. In terms of individuals, globalisation has created a situation where the boundaries between nationals and foreigners have all but been broken down. The fact that the 7 July 2005 London bombings were carried out by British citizens is irrelevant to whether they should be considered to be national security phenomena.

The same is true in terms of movements. Although the post 9/11 environment has tended to focus attention on a threat that has clear international elements, in many countries internal threats are the larger issue.

In many countries, national security is defined to include protection of the constitutional order and/or constitutional structures. Thus, the Hungarian National Security Services Act defines a national security interest as ensuring sovereignty and "safeguarding of the constitutional order".[26] In some cases, protecting senior government officials, such as the president or prime minister, is considered to constitute a national security activity.

It is not clear that the protection of these sorts of interests should always qualify as

[25] Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, 10 December 2008. Available at: http://www.cidh.oas.org/relatoria/showarticle.asp?artID=736&lID=1.

[26] Act CXXV of 1995, Section 74. Available at: http://href.hu/x/exu3.

a national security phenomenon. Thus, where an attack on a president was carried out by a single individual and motivated by hatred as opposed to a larger political purpose, it should probably be treated as an ordinary criminal matter. On the other hand, an attack on something as comparatively mundane as a bus station might qualify as a threat to national security if it were done by an organised group and was aimed at extracting political concessions. In other words, the factors noted above are probably more relevant than the specific target.

Defence of Other Countries and Humanitarian Actions

Technically, the defence of other countries is often not related to the security of the country undertaking the defensive action. This is even more the case where military forces are used for humanitarian actions, such as the current action in Libya. In many countries, national security is defined to include military plans, weapons systems and the like, regardless of what they may happen to be used for. Where this is the case, the defence of other countries through the deployment of military forces is automatically considered to fall within the scope of national security.

There is a certain logic to this. It would be difficult to separate out information that might threaten national security in the traditional sense and information that was limited to safety in relation to the specific (non-security) action. Thus information about weapons systems may need to be protected for purposes of other actions, whereas the timing of particular sorties would be more likely to be sensitive only in the context of the particular action. As a practical matter, separating out the information would probably be impossible, since it would require parallel systems of classification and information management for essentially the same information.

Specific Proposals

Preamble

These principles only apply in the context of national security claims by States that have a reasonable record of compliance with the rights set out in the Universal Declaration of Human Rights. In particular, they do not apply where States are seeking to use force to abuse human rights or to prevent democratic forms of participation.

Principle 2: Protecting National Security

(a) The right to information may be restricted only to protect specific interests as defined in international law, including national security.

(b) Restrictions on the right to information for purposes of the protection of national security may be applied only to information whose disclosure would be likely to materially harm the State's ability to prevent organised violent attacks that are motivated by a political, ideological or religious cause, and that are so serious that they require a national response, normally involving military action.

(c) The above applies to both internal and external attacks, and to attacks on other States and peoples, as well as the State invoking the restriction.

(d) A State may not invoke national security as a ground for restricting the right to information on the basis that this is necessary to contribute to its strength only through an impact on the economy, general welfare or similar considerations.

Note: In some countries, the conduct of foreign affairs is considered to be an element of national security. These Principles take the position that foreign affairs goes well beyond the scope of national security, but that the standards they posit may appropriately be applied to those aspects of foreign relations that promote national security as defined in this Principle and Principle 11.

Principle 11: Information That Legitimately May Be Subject to National Security Restrictions

(a) A State may only restrict the right to information on the basis of clear and narrow categories of information that have been listed in advance, and as necessary to protect legitimate national security interests, in accordance with these principles.

(b) A State may not classify or otherwise withhold information simply on the ground that it pertains to national security.

(c) Only information that falls into one of the following categories, and otherwise falls within the scope of national security as defined in Principle 2, may, in accordance with all of these principles, be restricted on national security grounds:

i. current military plans, order of battle information or operations;
ii. information, including technological data and inventions, concerning weapons and related systems, their production, capabilities, vulnerabilities or use;
iii. operational intelligence activities, sources or methods, including cryptology and the investigation of crimes, in connection with one of the other categories listed here;
iv. measures specifically designed to safeguard people, materials, systems or facilities against an attack which constitutes a threat to national security; or
v. information falling into one of the other categories listed here that was supplied by a foreign government with an express and written expectation of confidentiality.

Note: Information concerning the investigation or prosecution of terrorist acts may be

withheld on grounds other than national security, for instance, furtherance of the integrity or fairness of the investigation, prosecution or court proceedings.

Notes on These Proposals

i) The term right to information covers both the right to access information under an access to information law and the right not to be punished for disclosing information. This may need to be defined somewhere in the Principles.

ii) The reference to 'peoples' in Principle 2(c) is intended to cover foreign military actions that are humanitarian in nature.