

## **For a consistent policy in the struggle against proliferation networks**

**Guillaume Schlumberger & Bruno Gruselle**

(January 4 2007)

Proliferation networks operate like companies<sup>1</sup>. They must be capable of coordinating a series of elementary logistics, financial and technical functions.

Due to the increase in worldwide exchanges, the reinforcement of existing export control tools alone will not be sufficient to face the increase in proliferation flows. Despite widespread reporting in the media, interdiction operations<sup>2</sup> also can only have limited effect on networks, due to their occasional nature, if they are undertaken independently of an approach targeting other functions. It also seems hardly realistic to wish to neutralize a proliferation network only by freezing part of its credits in the framework of a repressive approach<sup>3</sup>.

Setting up an overall policy provides a means of coordinating intelligence actions, repression tools and interdiction means both nationally and internationally, and therefore appears as the only viable solution in the struggle against proliferation networks.

---

<sup>1</sup> B. Gruselle & G. Schlumberger. "Proliferation networks: between Sopranos and Supermarkets", FRS notes, July 2006.

<sup>2</sup> The interdiction consists of blocking ongoing transfers and operations. It may be done within a legal framework (seizure in customs, freeze account, sanctions) or militarily (interception of cargo at sea).

<sup>3</sup> Repression is intended to neutralize the activity of network agents or to prevent the completion of operations undertaken by them. For example, the objective may be to prevent access of the network to intermediate banks, to stop an intermediary or *a priori* to prevent the export of goods or transfer of technologies organized for the benefit of the network or one of its clients.

This is a complex task for it requires the organization of interministerial (or interagency) responsibilities, and in particular it requires an equilibrium between long term and short term actions. Finally, it depends on the reinforcement of links between the administrations involved and private participants including service companies, financial institutions and enterprises.

### **Intelligence, central tool in the struggle against networks**

The first step in an efficient struggle against proliferation networks is to carry out a mapping operation (network structure and operating modes) and requires intelligence capability in the various fields in which the networks are involved.

The network "mapping" work depends firstly on monitoring of flows, individuals and companies so as to detect proliferating activities. For example, monitoring of an identified intermediary in the Khan network provides a mean of finding supplier companies, intermediary banks and possibly other agents belonging to the network<sup>4</sup>. Two traps must be avoided in this approach; the temptation to stop an operation before the network has been fully characterized can be very strong, but it holds the risk of seeing it reorganize itself accompanied by the disappearance of participants who could have been observed so as to identify a key node<sup>5</sup>. *On the other hand*, failing to act before the network has been fully characterized can allow transactions to be completed with dramatic consequences in terms of dissemination of technologies.

Therefore an equilibrium has to be found between the need to obtain the most complete and detailed map possible and constraints to take action against a particular transaction or against a participant considered to be sufficiently important so that his neutralization will affect network activities in the long term<sup>6</sup>.

In terms of the national intelligence organization, the three large Western countries (United States, United Kingdom and France) have relatively similar tools; an internal security service and one or several organizations dedicated to abroad intelligence. This complete assembly can monitor activities of any networks on its own territory and their ramifications outside.

---

<sup>4</sup> <http://www.armscontrolwonk.com/1140/urs-tinner>

<sup>5</sup> The notes for the "Terrorism Financing and State Responses in Comparative Perspective" conference, Center for Contemporary Conflict, November 4-5, 2005, are particularly interesting in this question.

<sup>6</sup> The example of dismantlement of the Khan network is based on this equilibrium logic, American intelligence services probably having delayed action against the network so as to be able to act at the greatest possible depth.

Furthermore, financially the United States has created a structure that is distinctive in that it includes intelligence tools and means of taking action against networks, including internationally<sup>7</sup>. The Office of Terrorism and Financial Intelligence (OTFI) was created within the Treasury Department in 2004, and it has legal powers that enable the American government to target banks acting on behalf of networks<sup>8</sup>, and specific tools designed to monitor international financial flows. In particular, this arsenal<sup>9</sup> appears to include obtaining targeted data originating from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Finally, the functional concentration achieved within the Treasury department for financial security activities, enables the OTFI to obtain assistance from all services that might be concerned, including those originating from intelligence or financial repression activities.

In order to improve the efficiency of the intelligence function, it appears necessary to improve **dialog between services and small sensitive companies**; these are an attractive target particularly for networks, due to their economic vulnerability. The first step would consist of drawing up an exhaustive list of companies that might be concerned, and keeping it up to date. It would then be necessary to define the nature of exchanges between companies and intelligence services. For example, the American Treasury department performs an information mission before financial institutions in addition to advertising actions about cases for which repressive measures have been taken. Similarly, the TRACFIN unit receives declarations of suspicions but also in principle sends feedback to the declarer<sup>10</sup>.

---

<sup>7</sup> "Prepared Remarks by Stuart Levey, Undersecretary for Terrorism and Financial Intelligence before the American Enterprise Institute", September 8, 2006.

<sup>8</sup> This applies to:

- ❖ Executive Order 13382 June 28 2005 ("*Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters*"), enables the Departments of Justice, the Treasury and the State Department to prevent any transaction between the United States and persons or companies participating in proliferation activities. Section 5 authorizes the Treasury department to use these powers without prior notification to the persons concerned.
- ❖ Section 311 in the 2001 Patriot Act enables the Secretary of the Treasury to cut a foreign institution designated as being "of primary money laundering concern" from the American economic system.

<sup>9</sup> "Prepared Remarks by Stuart Levey, Undersecretary for Terrorism and Financial Intelligence before the American Enterprise Institute", September 8, 2006

<sup>10</sup> In two forms: information about processing of a specific declaration and information, training and targeted or untargeted awareness actions.

## How to neutralize networks?

### *Towards setting legal bases*

Since **resolution 1540 was adopted** by the United Nations Security Council in April 2004, efforts in the struggle against proliferation networks are backed up by a formal framework that fixes key measures to be taken by members of the organization in terms of:

1. **Interdiction of illegal intermediation activities** for weapons, vectors and related elements; in particular this is the purpose of item c) in article 3 that imposes that measures shall be taken to detect, dissuade, prevent and fight intermediation.
2. **Control of end users;** point d) in article 3 applies essentially to control of transit and transfers, but it also obliges States to set up means of controlling the nature of the end user.
3. **Control of services and funds** related to export operations; this particular point also obliges States to check "the supply of funds or services – for example financing or transport – related to export or transfer operations that contribute to proliferation".

However, it is regrettable that in terms of checking the service industry (transport, freighting, banks), resolution 1540 only recommends monitoring of activities related to exports *stricto sensu*. Furthermore, as a first reading, it is limited to criminalizing the proliferation of unconventional weapons carried out by non-State players<sup>11</sup>. Consequently, and even if the text is intentionally ambiguous concerning proliferation of WMD by States, its extension to this case would appear politically improbable; some countries legally pursue their activities for the development of nuclear weapons and *a fortiori* missiles.

**Resolution 1718, October 14 2006**<sup>12</sup>, voted following the North Korean test on October 9 2006, **could become a reference in the struggle against proliferation networks** to the extent that it is complementary to provisions of resolution 1540. Apart from giving UN members the right to freeze North Korean assets abroad, article 8.d states that States must prevent their nationals and persons operating within their frontiers from providing financial assistance to any person or entity involved in North Korean missile or nuclear programs. Article 8.f also decrees that all cargo entering or leaving the territory shall be searched. Application of this resolution, apart from its utility as an example for future or existing proliferation affairs, could help to improve methods used by some service companies who support operation of networks and possibly reinforce the dialog between the private sector and services and agencies responsible for the struggle against proliferation.

---

<sup>11</sup> See articles 1 and 2. Note that the application field is interpreted differently in different States.

<sup>12</sup> Voted under chapter VII.

Similarly, Security Council resolution 1737 imposing targeted sanctions on Iran<sup>13</sup> applies measures of the same nature to Teheran's nuclear program, targeting activities of institutions and intermediaries acting for the acquisition network. By setting up a committee responsible for its application, it opens up the possibility of modifying this list that takes account of the network's financial activities.

### *Widening the action field against proliferation networks*

Economic globalization makes it necessary to coordinate policies of States creating technologies and countries sheltering service activities<sup>14</sup> that could be used by organizations involved in the trade of weapons of mass destruction. Progress has undoubtedly been made since 2003 following the launch of the *Container Security Initiative* and the *Proliferation Security Initiative* in terms of cooperation on flow control. In particular, they have made it possible to set up systems for checking exports or goods in transit, in some States that acted as relays for network activities.

But genuine problems arise with the creation, and the use by States, of **lists of goods and technologies** for which export and transit are generally subject to prior authorizations. Complete systems and their main components are usually relatively well controlled because their end use is not questionable. On the other hand, the creation and updating of lists of dual-use goods can prove difficult considering constant changes of technologies<sup>15</sup>. For a country with limited administrative resources<sup>16</sup>, the volume of work involved in the management of export or transit applications (including transport documents<sup>17</sup>) for dual-use goods may become such that it introduces dysfunctions in their processing; delays, superficial analyses, errors, etc. Similarly, ill-informed or uninformed companies tend to submit incomplete or misleading demands to export control administrations.

However, a number of improvements could be considered:

- **Setting up of "catch-all" clauses.** The purpose is not to make a judgment about the intrinsic sensitivity of a product, but rather the intrinsic sensitivity of the end user and the possible use he might make of it<sup>18</sup>. "Catch-all" clauses also oblige exporters to inform control authorities about any suspicions they have about the end-use of the goods or the nature of the end user, thus contributing to making companies more responsible<sup>19</sup> (like the control over financial flows).

---

<sup>13</sup> <http://www.mideastweb.org/1737.htm>

<sup>14</sup> Financing, transport/freight, transfer, intermediation

<sup>15</sup> All that is necessary to be convinced of this is to look at the lists of goods produced by the Wassenaar arrangement.

<sup>16</sup> Precisely those for which vigilance is particularly desirable in terms of control to the extent that they are the main targets of networks.

<sup>17</sup> Cargo manifests in particular.

<sup>18</sup> Irina Albrecht, "Catch-all controls" paper prepared for the International Control Conference, London, 2004.

<sup>19</sup> Ibid. An example suspect declaration can be seen at:

- **The possibility of producing lists of suspect final destinations must be considered and generalized.** Such documents, despite the political difficulties that may surround their creation, have a genuine use in the context of the struggle against proliferation networks, provided that prior intelligence work has made it possible to map their structure. This is particularly true because production of this type of document may be envisaged within multinational groups<sup>20</sup>, so as to better coordinate efforts made by a group of countries.
- **Reinforcement of the required precision for transport documents** should be envisaged to prevent suspect and unusable declarations.

### *Struggle against financing of networks*

Even if its action is now concentrated on money laundering and financing of terrorism, the adoption of resolution 1540 **provides a basis for extending the scope of the international Financial Action Task Force (FATF<sup>21</sup>) to include the struggle against financing of proliferation.**

FATF recommendations apply essentially to the need for States to have a legal framework for tracking persons and legal entities involved in laundering activities and freezing their credits. Furthermore, the FATF proposes several ways of reinforcing the role of financing institutions in their struggle against laundering and financing of terrorism that could be interesting in terms of financing of proliferation.

### *Have legal tools to supervise the intermediary business*

**The generalization of provisions aimed at supervising the activities of brokers is becoming urgent.** Intermediaries play an important role in the operation of networks by acting as the main relays for acquisition attempts in other countries<sup>22</sup>. Apart from the United States that introduced provisions in 1996 related to brokers in the law on control of weapon exports<sup>23</sup>, few countries have any legal instruments that they can use against brokers<sup>24</sup>. However, there are some countries including

---

<http://www.bis.doc.gov/forms/eeleadsntips.html>

<sup>20</sup> For example for supplier groups: MTCR, NSG.

<sup>21</sup> The FATF was created in 1989 by the G-7, and now includes 33 member countries, this core being extended by observer countries and the existence of regional forums – for example an Asia-Pacific group to which China belongs – and the participation of international agencies or organizations.

<sup>22</sup> B. Gruselle & G. Schlumberger. "Proliferation networks: between Sopranos and Supermarkets", FRS notes, July 2006.

<sup>23</sup> Loretta Bondy, "The US law on arms brokering in 11 questions and answers", presentation to UN workshop in preparation of consultations on illegal brokering, May 2005.

<sup>24</sup> Note that American law makes authorization of brokering compulsory for all citizens of the United States, regardless of their country of residence.

France that have set up such tools. The European Union Council adopted a common position in 2003 on the control of armament intermediaries<sup>25</sup>. In both cases, the objective is to:

- List brokers operating on the territory concerned. It is sometimes envisaged to set up an activity authorization system, as a better means of controlling operators.
- Oblige intermediaries to obtain prior authorization for each operation in which they make a commitment.
- Set up a legal system punishing unauthorized intermediation activities.

### **Building a consistent interministerial and international structure**

The question of overall consistency must inevitably arise as new tools of different natures are added to the range of means designed to struggle against proliferation networks. The struggle against proliferation networks cannot depend on a logic of isolated and independent operations, it must form part of a coordinated international approach targeting all network functions.

There is no doubt that there is no organization or forum that has the task of precisely coordinating interception actions, possible financial operations and intelligence. The PSI provides an attractive framework for the creation of such an organization, because it already coordinates interception activities. However, *a priori* its operational and informal nature does not make it suitable for such a function. Therefore, it could be more useful to consider creation of an organization that would have the role of managing the use of all available tools to neutralize a specific network that would include the various administrations concerned, including Treasury, Customs, Defense and Intelligence services. The extent to which such an initiative could significantly improve the level and quality of intelligence exchanges essential for its operation remains to be seen.

---

<sup>25</sup> EU Council, "Position on the control of intermediaries in armament", 2003/468/CFSP, June 23 2003.

Finally, it is important to bear in mind that whatever measures and actions are taken to improve the struggle against proliferation networks, their economic impact on legitimate activities must be taken into account. In particular, it appears to be **essential to find a balance between the need for security and constraints related to international development of private players, at the risk of making measures that might be taken inoperative.**

*Opinions expressed in this document only commit the responsibility of their authors.*

