CO-CHAIRS' SUMMARY REPORT
ARF WORKSHOP ON PROXY ACTORS IN CYBERSPACE
HOI AN CITY, QUANG NAM PROVINCE, VIET NAM
14-15 MARCH 2012

1. Pursuant to the decision made by the 18th ARF on 23 July 2011 in Bali, Indonesia, the ARF Workshop on Proxy Actors in Cyberspace was held on the 14-15 March 2012 in Hoi An City, Quang Nam Province, Viet Nam. Mr. Vu Ho, Deputy Director-General, Ministry of Foreign Affairs of Viet Nam and Dr. Sharri Clark from the Bureau of Counterterrorism of the Department of State of the United States, co-chaired the Meeting.

2. Representatives from all ARF participants, except Brunei Darussalam, the Democratic People's Republic of Korea, Myanmar, New Zealand, Australia, Papua New Guinea, Sri Lanka and Timor Leste attended the Workshop. Representatives of the ASEAN Secretariat were also present. The Programme of Activities appears as **Annex 1**, and the List of Participants as **Annex 2**.

Session 1 – Opening Remarks and Introduction

3. Mr. Pham Quang Vinh, Deputy Minister of Foreign Affairs, ARF SOM Leader of Viet Nam, delivered his opening speech. He emphasized that the problem of proxy actors must be addressed, as it lies at the intersection of criminality and national security. He also stressed the importance of developing a common understanding of the problem, regional cooperation, and adherence to norms of behavior in cyberspace, grounded in national and international law. He suggested that the Workshop should foster capacity building and technical assistance and include best practices to help address the problem.

4. Dr. Sharri Clark in her welcoming remarks expressed appreciation to the Government of Viet Nam for co-chairing and hosting this Workshop. She briefly updated the Workshop on the United States' first *International Strategy for Cyberspace* introduced in May 2011, which describes the United States' approach to protecting cyberspace and ensuring that it promotes prosperity, security, and openness in the future. She noted that the capacity for states—perhaps states who do not possess the capabilities themselves—to enlist proxy actors to act on their behalf is a growing concern in cyberspace. To provide a basis for the discussion, she defined **proxy actors** as 'groups and individuals who, on behalf of a state (and possibly involving a state unwittingly), take malicious cyber actions against the governments, the private sector, and citizens of other states'. Dr. Clark noted that the workshop was intended to focus on proxy actors in cyberspace rather than on issues such as proxy servers or human rights advocacy. She recognized that the topic of proxy actors in

cyberspace is a new topic for most participants and that there are many aspects to the topic – including international policy, international law, and law enforcement. Nonetheless, she invited participants to actively engage in the discussions because it is an important issue that the participants need to work together to address.

Session 2 – The Threat of Proxy Actors in Cyberspace and the Role of Norms

5. Mr. Tom Dukes of the Office of the Coordinator for Cyber Issues, Department of State of the United States, discussed the evolution of the proxy actor threat and the role of international norms in addressing the threat. He briefly discussed what has been happening in the United Nations (UN) with regard to cyberspace, how states currently interact with each other in cyberspace and how cooperative measures—an accepted set of norms to address threats and vulnerabilities from technical, policy and legal standpoints--should be applied by governments in cyberspace. He noted that the 2010 UN Secretary-General's Report on the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement) identified proxy actors as an issue that states should address and international cooperation between states as one of the key means to do so. Mr. Dukes recapped some recommendations, including further dialogue among states, capacity building, especially with regard to cybercrime, and developing CERTs and other emergency response capabilities that can cooperate nationally and internationally. He also shared the United States' efforts in addressing cyberspace issues, including its *International Strategy for Cyberspace* (http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf), introduced by President Barack Obama in May 2011. He added that the United States is not the only country to publish its views and structures to put them in place, including appointing officials at high levels to deal with cyber issues, but that these measures force states to think about their positions on cyber issues and to get commitment at the highest political levels. Mr. Dukes noted that the UN report states that much work has been done on cyber issues in regional organizations, specifically the ASEAN and the ARF. He suggested that this Workshop should be used as an opportunity to exchange experiences and views with regard to the development of international norms for interaction between states in cyberspace, as new areas where there is no consensus view such as this need robust dialogue. On this matter, Mr. Dukes reiterated that the United States is committed to working closely together with like-minded states on peaceful conduct in cyberspace.

6. The second panellist of this session, Dr. Tran Van Hoa, Deputy Director of the Viet Nam High-Tech Crime Policy Department, discussed the tools and methods used by proxy actors and problems with attribution, trends in cybercrime in Viet Nam and initiatives by Viet Nam to address issues pertaining to cyber security. Dr. Hoa elaborated on types of proxy servers that are commonly used. He emphasized that it is important to identify servers used in order to identify and prosecute proxy actors. He also mentioned that in 2009, Viet Nam amended its Penal Code with the introduction of five new articles related to cybercrime. This is the basic legal foundation for law enforcement agencies to effectively prevent and suppress cybercrime. To deal with cybercrime, he stressed the need to intensify the exchange of information and experiences among the ARF participants and to promote ARF cooperation on cybercrime investigation, as well as training for law enforcement agencies in developing countries on cybercrime investigation and data recovery. Dr. Hoa's presentation appears as **Annex 3**.

7. The Workshop deliberated on the difficult issue of attribution, especially on methods to identify the (possibly proxy) actors behind the activities and possible solutions to address these threats. The most important aspect of investigating any crime, including cybercrime, is evidence that allows the identification of a specific person behind the crime. In the context of proxy actors in cyberspace, identification of the actor(s)--and whether they are acting as proxies for state or others--are critical issues. The Workshop was also reminded that there is an increase of both intentional and unintentional safe havens for illegal proxy actors. The Workshop exchanged views on how governments deal with the issue of attribution. It was noted that there are no right or wrong answers in dealing with the issue, as it all depends on each country's legal and political systems. However, the Workshop also agreed that the ultimate goal is to reach agreement on high-level norms of behaviour and principles that all governments should adhere to in order to deal with this problem.

8. The Workshop noted the challenges faced by ARF countries in identifying the perpetrators of illegal proxy actors, among others:

    a. proxy actors can use IP addresses of other countries outside their own;
    b. IP addresses used by proxy actors can change repeatedly, thus it is difficult to trace the origin of the user;
    c. there may be technical, legal and/or political difficulties in gathering digital evidence (particularly when multiple countries are involved); and
    d. proxy actors and evidence may be located in multiple countries.

9. The Workshop agreed that developing a strong network of cooperation among law enforcement agencies, both formal and informal, is vital in the area of cybercrime. The existence of a rapid assistance mechanism is

also important to enable the recognition of physical evidence such as computer log files, which are files containing vital information on detailed computer activity that is only accessible for a short period of time before it is overwritten or deleted. The Workshop observed that without close cooperation with other countries, investigations to tackle the problem of attribution in cybercrime incidents often ends abruptly. Therefore, it was also agreed that there is a need for a high-level policy-making body in each government in order to address these problems. An example of strong cooperation is the exchange of information on cases where an IP address from country A is being used as a "hopping point" for activities originating from an IP address in country B. The Workshop noted that several mechanisms for law enforcement networking have been established, such as the G8 24/7 Network and the G8 High Technology Crime Subgroup, national Computer Emergency Response Teams (CERTs), and the mechanisms laid out by the Budapest Convention (http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185 &CL=ENG). Some ARF participants discussed national regulations on proxy actors as an alternative to the bureaucracy of mutual international legal cooperation and assistance.

10. The Workshop discussed how to securely communicate and keep information restricted with regard to proxy actors' activities, for example among the South Asian Association for Regional Cooperation (SAARC) members. Several cyberspace-related crimes that are commonly found in the SAARC region were identified, namely computer intrusion, data theft, credit card fraud, telecommunication fraud, money laundering, child pornography and special software privacy. Investigating terrorism is typically complicated by classification issues. It was noted in the Workshop that international law enforcement communities are more advanced in securely communicating among themselves. Their networks, aside from being secure, are also very instructive. One example of an existing law enforcement communication network is the 24/7 Network which operates in 60 countries worldwide. Each country identifies a single national point of contact. If a country sees malicious activity coming from another country in the network, it can contact the designated point of contact in that country and request information such as the IP address involved in the attack. Since connections have been established through the network, the country knows that it is credible information and feels comfortable sharing information through those channels. To increase effectiveness in sharing information, the network may bring together national points of contacts in conferences, run PING tests every three to four months and carry out exercises to make sure the network is running smoothly. Other networks do the same thing informally, such as the network of INTERPOL members. Outside of law enforcement networks on criminal matters, state-to-state communication is more difficult. However, the nuclear arms nonproliferation framework is a good model.

The basic concepts of this kind of framework can and are being applied on the issue on cyberspace as Confidence-Building Measures (CBMs) or ways in which countries can ensure communication with each other without misunderstandings. Some participants in the Workshop suggested that countries that have less connectivity to the internet tend to think that these issues are less important to them. They also have the advantage of being able to learn from others' mistakes in combating cybercrime.

11. The Workshop agreed that internet crimes are borderless, faceless and transnational. Although strong cooperation is vital, the Workshop debated whether it is important to develop an international law enforcement body on the model of INTERPOL to deal with internet crimes and/or to establish an agreement on what constitutes an internet crime, as this differs in different countries. The Workshop further noted that countries take different approaches to tackling cybercrime. However, the ARF participants agreed on the need for an international agreement on what constitutes a cybercrime, the challenge being getting all countries to agree that certain conduct constitutes an offence. This would take at least a decade. Meanwhile, countries need to move fast in responding to criminal threats in cyberspace, and the Workshop noted that the Budapest Convention is a good framework and approach in addressing cyberspace-related issues. In addition to being parties to international agreements, it is important for countries to first put in place national laws that are necessary to effectively tackle cybercrime.

12. The Workshop noted the suggestion of one ARF participant that since proxy actors in cyberspace pose a serious threat, an international legal instrument or treaty (such as a "code of conduct" that they have proposed), or even an international organization affiliated with the UN ITU or INTERPOL that is dedicated to combat these kinds of activities, is needed. The ARF participant then proposed five basic principles to be discussed for further development of international norms of behaviour with regard to proxy actors in cyberspace, namely: 1) cyber sovereignty (nations having jurisdiction over their domains); 2) international cooperation (common responsibility); 3) balance between online freedom of expression and cybersecurity; 4) peaceful use of the internet for international stability; and 5) equitable development and assistance in capacity building.

13. The Workshop also noted recent developments in cybersecurity in the private sector. For example, it was noted that there is a huge increase in the volume of financial transactions being done through cloud computing. Major IT companies such as Microsoft and Huawei, among many others, are using this technology. There is growing concern about protecting the high volume of transnational financial and other transactions from cybercrime.

Session 3: Legal Frameworks for Proxy Actors in Cyberspace

14. Mr. Phillip Spector of the Office of the Legal Adviser, Department of State of the United States, delivered his presentation on legal principles and international legal frameworks that may be relevant in considering the issues posed by proxy actors in cyberspace. He presented case studies, which framed the discussion of states' responsibilities regarding proxy actors and the international legal implications. The case studies may set precedents outside of the cyberspace context that deal with state enlistment of proxy actors, including:

    a. The Case of the Republic of Nicaragua v. the United States of America in 1986 where the International Court of Justice (ICJ) issued a landmark ruling against Nicaragua and in favour of the United States, based on the fact that Nicaragua had failed to show "that that State had **effective control** of the military or paramilitary operations in the course of which the alleged violations were committed" for the contras' actions to lead to legal responsibility on the part of the United States for all of its acts; and
    b. The ICJ case of Bosnia and Herzegovina v. Serbia and Montenegro in 2007, which considered the Application of the Convention on the Prevention and Punishment of the Crime of Genocide. The Court found that Serbia was neither directly responsible for the Srebrenica genocide, nor complicit in it because they had been perpetrated by entities, groups and individuals within Bosnia over whom Serbia (at the time, the Federal Republic of Yugoslavia) did not maintain a sufficient degree of control.

15. Mr. Spector noted that the conduct of a person (or proxy actor) is not always attributed to the state, and the state is not always responsible for the acts of a person (or private party). However, in ruling on cases of state attributions, the thread of international customary law must be observed, and a state cannot hide behind a person or a group of persons in carrying out unlawful acts. A state can be responsible for a private act if the following conditions are met:

    a. a states' level of involvement goes beyond encouragement and financial support;
    b. a state has specifically directed the person(s) to do something or issued instructions; and
    c. a state has exercised effective control over those person(s), all in breach of international law.

Therefore, a state can be held responsible for its control of proxy actors, if these conditions are met. Of course, non-state actors can enlist proxy actors as well. Mr. Spector's presentation appears as **Annex 4**.

16. Mr. Masashi Horie from the International Legal Affairs Division, Ministry of Foreign Affairs of Japan, outlined the existing basic international legal frameworks and other rules of international law relevant to proxy actors. In addition to the attribution criteria, some affirmative rules under existing international law were also mentioned. He cited ICJ judgments on cases such as the Corfu Channel Case and the 1979 case between Iran and the U.S. Diplomatic and Consular Staff in Tehran. Mr. Horie noted that every state has obligations and that when a state is aware of malicious activity in another state, it has responsibilities. Otherwise, it is a breach of international obligation.

17. The Workshop deliberated the responsibility of the state regarding private individuals or groups engaging in criminal cyberspace activities and forms of cooperation between states. The Workshop also reflected on the role of the ICJ in settling cases related to cybercrime that affect interstate relations, and considered how this might extrapolate to proxy actors in cyberspace.

18. The Workshop noted that legal frameworks rely on evidence being collected -- and that there are challenges in collecting evidence of cybercrime cases that move across borders at the speed of light. The Workshop further discussed the possibility of developing a system to enable the collection of evidence to support better investigation in cyberspace, citing the example of the financial sector's handling of proxy actors within their realm. The Workshop agreed that evidence collection is a critical factor in addressing cybersecurity.

19. The Workshop noted that although private actors in cyberspace are not inherently bad and some uses of proxy actors can be acceptable, the issue is the use of proxy actors by states to commit acts that are illegal under international law. . The Workshop agreed that dealing with proxy actors requires careful investigation, because this could mean dealing with the indirect behaviour of states. The Workshop deliberated about organizations that have the legitimacy to find or trap proxy attackers. Some participants suggested that there should be an organisation affiliated with the UN so it would have legitimacy to tackle the issue. However, the international community has developed some bodies already effective at resolving these issues. For states with advanced technology such as China, the United States or Japan, retaliation for attacks could be large in scale. States could enlist proxy actors to increase the scale of their retaliation, which could do more damage than the original attack. The Workshop observed that it is a great challenge to find the

person behind an attack because attackers can use many means to hide their IP addresses. Some technologies such as anonymizers can be used positively for privacy, but can also be misused.

20. The Workshop exchanged views on what constitutes a wrongful act and how a state may be held responsible for the acts of the proxy actor in cyberspace without disregarding the state's sovereignty. These issues need further discussion, and consensus between states is needed, which takes time. Another important issue to address is how to determine and prove whether an act is indeed an act of a state by looking at the intent of the state—although proving intent may be difficult. However, if the state doesn't know that a private actor has engaged in the wrongful act, then the state should not be held liable.

21. The Workshop discussed whether there is a need to agree to judgment by a third party, for instance by establishing a body like the ICJ. The Workshop agreed that at this point it may not be necessary to have a new doctrine or legal body, since most disputes have been resolved in the ICJ and the International Criminal Court (ICC).

22. The Workshop concluded that the most important thing to do in preventing cybercrime is to identify the parties responsible for the attacks in cyberspace—whether an actor, a state, or both. States need to come to a common understanding regarding what needs to be done and must have the political will to cooperate with each other. The Workshop expressed its view that the ARF should explore ways to promote these efforts.

Session 4 – Strategies for Dealing with Cybercriminals as Proxy Actors in Cyberspace

23. Mr. William Hall from the Computer Crime and Intellectual Property Section (CCIPS), Department of Justice of the United States, delivered his presentation focusing on how the criminal model operates and scenarios involving proxy actors. He emphasized that the Budapest Convention is an important instrument because it covers most of the criminal activities in cyberspace, including preservation of evidence and international law enforcement cooperation. The bedrock principle of the Convention is dual criminality, which suggests that an incident has to be regarded as a crime in both countries for law enforcement cooperation to be able to take place. Thus, it requires the signatories of the Convention to pass national laws to give prosecutors the confidence that a certain act is also a crime in the other country. He also explained scenarios involving proxy actors to determine whether or not the international criminal model works with the proxy actor situation. He mentioned the following most common scenarios:

a. if the proxy actor is committing a crime inside the victim state, the victim state's domestic laws can be used to process the case, and as the evidence will be located within the victim state it will be easier to seize the evidence;
b. if the proxy actor is committing a crime inside the supporting state, and the victim state is seeking evidence from the supporting state, evidence collection may be difficult (the Budapest Convention would be helpful); and
c. if evidence and proxy actors are in a third party state, or the proxy actor is in one state, but the evidence is in many different states, the third-party country that is being asked for evidence really has nothing to do with the case. Still, it is important for that state to cooperate in the investigation, especially with the victim state (the Budapest Convention would be helpful). An outline of Mr. Hall's presentation appears as **Annex 5**.

24. Professor Dato' Bin Jazri Husin, CEO of Cyber Security Malaysia, presented on the topic of capacity building. He pointed out that there is a huge threat in fitting in the digital world into a previously 'traditional world'. The key factor for success for all government initiatives regarding proxy actors is the effectiveness of the capacity building programs and the cooperation between parties in collecting and analyzing evidence. Capacity building can be done through government and private sector relationships and also be undertaken by higher institutions. An example of concrete capacity building initiatives is the creation of centres of excellence that can be replicated in ARF countries for the training of experts in cybersecurity. He noted that one objective of centres of excellence supported by all is to build trust and competencies. He mentioned that Malaysia is more than willing to volunteer in helping create the initial model and is asking for joint partnership to develop, create and design a centre of excellence that focuses on the expertise needed. Pakistan offered to work with Malaysia on developing a centre of excellence, and other ARF participants echoed the importance of the concrete step of capacity building for developing nations.

25. The Workshop took note of the other ARF participants' views on the Budapest Convention as the key instrument because it is the only international instrument we have dealing with cybersecurity issues in the near future. It is a good guideline for the purpose of developing national legislation. Capacity building is another key issue and the Council of Europe working with the private sector has a programme called the Council of Europe Global Project on Cybercrime. The EU has already worked with technical capacity programmes, and examples of these programmes might be of interest to the ARF. Other ARF participants noted that even the Budapest Convention hinges on capabilities, which is a hindrance to developing countries and suggested that it is dated and has

some gaps. However, the Workshop noted others' views that countries can use it as a template tailored to their own criminal and legal systems.

26. The Workshop underscored that capacity building should be one of the main agendas for the cyberspace issue. The Workshop also recognized that there is no programme that specifically addresses proxy actors and that it is possible to have experts from certain countries such as China, Korea and Japan share their expertise with the rest of the ARF participants. It was stressed that trust-building between countries is very important to working together to tackle cybercrime.

27. The Workshop agreed that almost all countries are using information and communications technology (ICT) as a platform for development. Even countries that are lagging behind are trying to come up with national legislations and legal framework. Thus, legal and institutional frameworks are needed for the sustainability of combating cybercrime.

28. The Workshop exchanged views on the need to develop a new convention under the UN framework to complement the Budapest Convention. As the Budapest Convention was drafted a decade ago in the late 1990s and adopted in 2001, some participants were of the view that the Convention is unable to address all cybercrime-related acts in some developing countries. On the other hand, it was also noted that the Budapest Convention is not the sole instrument to be used for cybercrime. It provides a framework for other processes. While the Convention does not cover all conceivable acts related to cybercrime, countries that recognize crimes not covered may wish to support the Convention with their own national law. The Budapest Convention is not outdated. In fact, more countries such as Australia, Japan, and also developing countries such as Senegal and the Dominican Republic are trying to become signatories. Others have used the Convention as a model. For example, based on the Convention, the African Union is currently developing a Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

Session 5 – Wrap-up and the Way Forward

.

29. Mr. Vu Ho discussed some conclusions from the Workshop, including the need to step up cooperation within the region, including legal cooperation, the need for capacity building to close gaps in capabilities between ARF participants in the region, and the need to promote norms of behaviour in cyberspace in the region. He noted that since 2005 the ARF has worked on cyber issues, but that it is now time for ARF to explore deeper issues in this area.

30. Mr. David Hamilton, Deputy Director of the International Crime and Terrorism Division, Foreign Affairs and International Trade Canada,

discussed the Workshop in the context of advancing the ISM-CTTC's objectives, including ICT security. He noted that transboundary threats such as cyber threats require multistate responses, so the norms of behaviour in cyberspace and capacity building discussed in this Workshop will be useful for ARF's future work.

31. The Co-Chairs concluded the Workshop and thanked the participants for their active engagement in the Workshop, which was convened for the first time to specifically address the important issue on proxy actors in cyberspace. It was underscored that the Workshop has resulted in generating awareness and common understanding regarding the roles of the proxy actors as well as their tools and methods. The Workshop also commended the sharing of experience, which is very useful for all ARF participants. Finally, the Workshop viewed building international norms of behaviour in cyberspace as very important.

32. The Workshop noted the following specific recommendations for a way forward for the ARF to address issues such as proxy actors in cyberspace in the context of promoting norms of behaviour in cyberspace:

    a. Expand the role of the ARF as the primary security forum in the region to explore deeper issues related to cybersecurity;
    b. Explore new avenues for cooperation;
    c. Step up cooperation in the area of combating cybercrime, including crimes by proxy actors in cyberspace;
    d. Continue promoting confidence-building measures to ensure regional security and stability;
    e. Promote and create an environment conducive for all parties and countries to step up their efforts in cybersecurity;
    f. Explore the possibility of establishing an ARF plan of action on cybersecurity;
    g. Set up a database of experts on proxy actors in cyberspace and other cyber issues from each ARF participant in this region to be sent to the ARF Unit of the ASEAN Secretariat; the ARF Unit could take input from all countries and share the database on the ARF website develop a database of experts on proxy actors and other cyber issues in the region and provide it to the ARF Unit for its website;
    h. Continue discussing the issue of proxy actors in cyberspace in the future;
    i. Organize cybersecurity capacity building courses for all countries in the region;
    j. Step up public awareness of cybersecurity in all countries in this region; and
    k. Set up common approaches by countries in the region to handle this problem.

33. The Workshop expressed gratitude to Viet Nam and Canada for their co-chairmanship of the ARF. They also thanked the Government of Viet Nam for their generous hospitality and excellent arrangements in hosting the ARF Workshop on Proxy Actors in Cyberspace.

■■■■