## Code: Resolution 1-1 Committee: Security Council Subject: *Enhancing International Cooperation of the Implementation of Counter-terrorism*

1 *Recognizing* the irreplaceable importance of United Nations Security Council Resolution 2 S/RES/2082 and S/RES/2083 of 2012 and viewing the Global Counter-terrorism Strategy at the 3 most comprehensive way to consolidate the international community and help to enhance global 4 counter-terrorism efforts, 5 6 Recalling the United Nations Counter-Terrorism Implementation Task Force (CTITF) and the role that 7 it has played in providing practical, implementable measures to the international community for the 8 purpose of combating terrorism in all of its stages and forms, 9 10 Gravely aware that there has been an undeniable rise in the level or organization and improved material-11 technical support of terrorist organizations, as well as the expanded social base of terrorism and the 12 increased severity of consequences and the number of causalities, 13 14 *Reminds* member states that actions in opposition to the UN Charter and mandates created by the UN 15 Security Council fall within the realm of non-compliance, 16 17 *Expressing its appreciation* of existing counter-terrorism agencies such as the Counter-Terrorism 18 Committee and their efforts in recognizing and combating terrorism in all of its forms and 19 manifestations, 20 21 *Reaffirming* current regional organizations that have over time evolved to become counter-terrorism 22 collaborations such as, but not limited to, NATO, Tri-Lateral Tri-Border Area Command, and the 23 Shanghai Cooperation Organization as effective examples regarding preventative measures towards 24 combating international terrorism, 25 26 Acknowledging the increasing transfer of financial assets and material-technical support between states 27 and known terrorist organizations that result in the increased threat posed to international peace and 28 security, 29 30 Noting with deep concern previous actions taken by states in regards to the aiding and abetting of 31 international terrorists within their borders, 32 33 The Security Council, 34 35 1. Authorizes the utilization of a three-tiered system, in which counter-terrorism efforts are addressed on 36 a state, regional, and if ultimately needed, an international level which: 37 38 a. Allows for Member States to protect the safeguard and security of their borders, 39 emphasizing the principles of sovereignty, 40

41 42	b.	Increases development of military independence and law enforcement infrastructure for the purpose of allowing states to effectively protect their borders against terrorist	
42 43		attacks,	
44		attacks,	
45	с.	Utilizes regional level aid should they be unable to adequately combat terrorism at the	
46	с.	state level,	
40 47		state rever,	
48	d.	Endorses states to utilize regional frameworks if currently established,	
49	u.	Endorses states to utilize regional frameworks if currently established,	
<del>5</del> 0	e.	Increases work done toward consistent, reliable, and regularized information-sharing	
50 51	с.	among private sector and governments with particular emphasis on infrastructure	
52		protection,	
53		protection,	
54	f.	Allows Member States without a counter-terrorism framework to develop similar	
55	<i>J</i> •	organizations specifically for the purpose of security-related issues,	
56			
57	g.	Hold their member states in regional organizations accountable for pursuing counter-	
58	0.	terrorism efforts by requiring annual reports to the regional body,	
59			
60	h.	Reminds states to call upon the UN Security Council in circumstances where the regional	
61		body is unable to comprehensively address its duties of maintaining stability,	
62			
63	i.	Assigns the responsibility of international peace and security to its members,	
64			
65	<i>j</i> .	Authorizes the Security Council within the aforementioned three-tiered strategy in the	
66		case of the exhaustion of alternative options, and	
67			
68	<i>k</i> .	Evaluates, analyzes and addresses each respective issue presented on an individual basis;	
69			
70	2. Strongly condemns the aiding and abetting of terrorists and terrorist organizations by states and non-		
71	state actors an	d further presses member states to implement monetary and armament sanctions against	
72	said states or	non-state actors;	
73			
74	3. Affirms that states and organizations who provide aid in the form of funding, or provisions of weapons		
75	to terrorist organizations be considered a threat to international peace and security and therefore become		
76	subject to monetary and armament sanctions;		
77			
78	4. Decides to	remain actively seized on the matter.	

*4. Decides* to remain actively seized on the matter.

Code: Resolution 1-2 Committee: Security Council Subject: *Enhancing International Cooperation on the Implementation of Counterterrorism* 

1 2 3 4	<i>Recognizing</i> the current working definition of terrorist acts in United Nations Security Council (UNSC) Resolution S/RES/1566 (2004) and the mandate of the United Nations Counter-Terrorism Implementation Task Force (UN CTITF),		
4 5 6	In accordance with previous UNSC Resolution 1373 (2001),		
7 8 9	<i>Deeply concerned</i> with the fact that the international trend of acts of terrorism has increased by 10,000 acts over the past three decades according to the 2011 United States Country Reports on Terrorism from The National Counter-Terrorism Center,		
10 11 12 13	<i>Recognizing</i> the growing threat of novel forms of terrorism that have emerged since the inception of S/RES/1566 (2004),		
13 14 15 16 17 18	<i>Citing</i> the requirements set by the United Nations Financial Action Task Force (UN FATF) within the Anti-Money Laundering and Countering Terrorist Financing standards and the authority granted to the Security Council through Chapter 6, Article 37, Part II of the United Nations Charter,		
19 20 21 22	Acknowledging the growing nuanced threat of cyber terrorism perpetrated by both state- sponsored entities and non-state actors and the need for greater exchange of pertinent operational information,		
22 23 24	Acting under Chapter VI Article 33 and 34 of the United Nations Charter,		
25 26	The Security Council,		
27 28 29 30	1. <i>Emphasizes</i> the enhancement of collaboration in the existing counterterrorism committees, such as the CTC as per UNSC Resolution 1373 and the Counter-Terrorism Executive Directive is essential in the effort to combat terrorism through:		
31 32	a. The maintenance of terrorist databases to a higher level of standard,		
33 34 35 36	b. Broadening the "Al-Qaida Sanctions Committee" to focus not only on the Al- Qaeda terrorist organization but also those that fall under the inclusive definition of terrorism, and		
37 38 39	c. The enhancement of information sharing between states of the international community pertinent to terrorist activities;		
40 41	2. <i>Advocates</i> the creation of a comprehensive counterterrorism forum for voluntary Member States in the areas of law enforcement, military capacity building,		

<ul> <li>a. Which will be hosted by rotating Security Council Member States to foster international cooperation on an ad hoc basis,</li> <li>b. In conjunction with the UN CTC,</li> <li>c. To advocate the inclusion of humanitarian protocols within these measures in accordance with the Millennium Development Goal Two;</li> <li>3. <i>Recommends</i> Member States to comply with requirements established by the Anti- Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Anti- Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li>4. <i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. <i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>E</i></li></ul>	42 43		intelligence agencies, emergency services coordination, and raising public awareness of terrorism prevention:
<ul> <li>b. In conjunction with the UN CTC,</li> <li>c. To advocate the inclusion of humanitarian protocols within these measures in accordance with the Millennium Development Goal Two;</li> <li>3. Recommends Member States to comply with requirements established by the Anti-Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li>4. Encourages international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to access information in midst of a cyber-attack,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>d. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>	45 46		
<ul> <li>c. To advocate the inclusion of humanitarian protocols within these measures in accordance with the Millennium Development Goal Two;</li> <li>3. <i>Recommends</i> Member States to comply with requirements established by the Anti-Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li>4. <i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. <i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyberattack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>	48		b. In conjunction with the UN CTC,
<ol> <li><i>Recommends</i> Member States to comply with requirements established by the Anti- Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li><i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ol>	50		-
<ul> <li>Money Laundering/Countering the Financing of Terrorism (AMC/CFT) standards, with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li><i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>		2	
<ul> <li>with particular emphasis on Recommendation 20, as established by the Financial Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li><i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>		3.	
<ul> <li>Action Task Force (FATF), which calls upon Member States to report suspicious financial activity to the FATF;</li> <li>4. Encourages international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>financial activity to the FATF;</li> <li><i>Encourages</i> international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>4. Encourages international regulatory agencies and relevant regional groups to freeze and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>	57		
<ul> <li>and seize assets of proven terrorist financiers in order to acknowledge regional and international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>international consequences of terror attacks on the international political economy and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>		4.	
<ul> <li>and the wider implications upon international trade, business practices, and general welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			1 0 0
<ul> <li>welfare;</li> <li><i>Suggests</i> that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>5. Suggests that the Member States' governmental institutions update their current cyber security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. Emphasizes a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			wenale,
<ul> <li>security mechanisms so that their servers push all data in regularly appropriated intervals as well as requesting the Member States to create backup server networks:</li> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>		5.	Suggests that the Member States' governmental institutions update their current cyber
<ul> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>a. That update themselves by push sync from a main server in specific intervals following approval from said server network, and kept offline to ensure insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>	67		intervals as well as requesting the Member States to create backup server networks:
<ul> <li>following approval from said server network, and kept offline to ensure</li> <li>insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber-</li> <li>attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber</li> <li>Threats (IMPACT) be involved with the advisement of said server backups as</li> <li>well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>insulation from cyber threats,</li> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>b. That allows for Member States to access information in midst of a cyber- attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			insulation from cyber threats,
<ul> <li>attack,</li> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber</li> <li>Threats (IMPACT) be involved with the advisement of said server backups as</li> <li>well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			b That allows for Member States to access information in midst of a cyber-
<ul> <li>c. That only grant client-access to said Member State, or civil society, and</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			· · · · ·
<ul> <li>77</li> <li>78</li> <li>d. Recommends that the International Multilateral Partnership Against Cyber</li> <li>79</li> <li>79</li> <li>79</li> <li>79</li> <li>70</li> <li>70</li> <li>70</li> <li>71</li> <li>71</li> <li>72</li> <li>73</li> <li>74</li> <li>75</li> <li>76</li> <li>77</li> <li>78</li> <li>79</li> <li>79</li> <li>70</li> <li>70</li> <li>71</li> <li>71</li> <li>72</li> <li>74</li> <li>75</li> <li>76</li> <li>76</li> <li>77</li> <li>78</li> <li>79</li> <li>79</li> <li>70</li> <li>70</li> <li>71</li> <li>71</li> <li>72</li> <li>74</li> <li>75</li> <li>76</li> <li>76</li> <li>77</li> <li>78</li> <li>79</li> <li>79</li> <li>70</li> <li>70</li> <li>71</li> <li>71</li> <li>72</li> <li>74</li> <li>75</li> <li>76</li> <li>76</li></ul>			
<ul> <li>d. Recommends that the International Multilateral Partnership Against Cyber Threats (IMPACT) be involved with the advisement of said server backups as well as having quarterly meetings with the CTC;</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>a. State level management as a first response,</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>	76		c. That only grant client-access to said Member State, or civil society, and
<ul> <li>79 Threats (IMPACT) be involved with the advisement of said server backups as</li> <li>80 well as having quarterly meetings with the CTC;</li> <li>81</li> <li>82 6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>83</li> <li>84 a. State level management as a first response,</li> <li>85</li> <li>86 b. Regional responsibilities should the state level management fail, and</li> </ul>	77		
<ul> <li>80 well as having quarterly meetings with the CTC;</li> <li>81</li> <li>82 6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>83</li> <li>84 a. State level management as a first response,</li> <li>85</li> <li>86 b. Regional responsibilities should the state level management fail, and</li> </ul>			
<ul> <li>81</li> <li>82</li> <li>6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>83</li> <li>84</li> <li>84</li> <li>85</li> <li>86</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>			· · · · · · · · · · · · · · · · · · ·
<ul> <li>82 6. <i>Emphasizes</i> a three tier process in conflict management that involves the:</li> <li>83</li> <li>84 a. State level management as a first response,</li> <li>85</li> <li>86 b. Regional responsibilities should the state level management fail, and</li> </ul>			well as having quarterly meetings with the CTC;
<ul> <li>83</li> <li>84</li> <li>85</li> <li>86</li> <li>b. Regional responsibilities should the state level management fail, and</li> </ul>		6	Emphasizes a three tier process in conflict management that involves the
<ul> <li>84 a. State level management as a first response,</li> <li>85</li> <li>86 b. Regional responsibilities should the state level management fail, and</li> </ul>		υ.	Emphasizes a unce del process in conflict management dat involves de:
<ul><li>85</li><li>86</li><li>b. Regional responsibilities should the state level management fail, and</li></ul>			a. State level management as a first response.
b. Regional responsibilities should the state level management fail, and			······································
87			b. Regional responsibilities should the state level management fail, and
	87		

- 88 c. Invoking Security Council jurisdiction should regional crisis control fail;
- 8990 7. *Decides* to remain actively seized in the matter.



## Statement by the President of the Security Council Regarding the Situation in the Democratic Republic of Congo

At the Security Council meeting held on 27 October 2013, in connection with the Council's consideration of the situation in the Democratic Republic of the Congo, the President of the Security Council makes the following statement on behalf of the Council:

"The Security Council is deeply concerned by the current situation in the DRC, and stresses the importance of responsibility to protect the population of its population.

"The Security Council condemns the escalating violence perpetrated by Movement 23 rebels in the Democratic Republic of the Congo and seeks to immediately address the humanitarian and refugee crisis.

"The Security Council, referencing SC Resolution 2098 (2013) and the Responsibility to Protect (R2P), seeks immediate action in the form of the following strategy.

"The Security Council agrees to develop, in the next fifteen days, the explicit rules of engagement for MONUSCO troops in the region with substantive efforts from the French-led NATO forces with technical and logistical assistance from the Shanghai Cooperation Organization to regain control of the airport in Goma.

"The Security Council, forming a diplomatic approach towards the conflict in order to prevent further loss of life and maintain sustainable peace, asks the assistance of the Peace and Security Council of the African Union to contribute its own peacekeeping forces to the stabilization efforts in the DRC.

"The Security Council agrees to send, in the next fifteen days, an immediate exploratory investigation of the situation and circumstances including foreign involvement currently surrounding the conflict in the Democratic Republic of the Congo take place in order to allow for a more complete picture of the conflict and for the Council to better evaluate the most effective and longstanding method to pursue further action regarding the situation. "The Security Council calls on All Member States to implement the sanctions with the accordance of the previous SC resolutions, in particular resolutions 1493 (2003), 1533 (2004), 1596 (2005), 1649 (2005), 1698 (2006), 1768 (2007), 1771 (2007), and 1799 (2008), as well as the recent resolution that this Council passed, resolution 1-1."

"The Security Council reiterates its strong condemnation of terrorism in all its forms, committed by whomever, whenever, or whatever purposes, and stresses that any terrorist acts are criminal and unjustifiable regardless of their motivation.

"The Security Council reaffirms its primary responsibility for the maintenance of the international peace and security, in accordance with the Charter of the United Nations.

