Thresholds for Cyberwar
James A. Lewis, Center for Strategic and International Studies
September 2010SIS

There is a broad range of hostile or malicious action in cyberspace – crime, espionage, attacks, and political action. The identity of those who engage in these actions can be indeterminate, and these activities, at some level, often overlap. This does not justify, however, a similar blurring and imprecision in our discussions of cyber conflict. We can reduce this blurring by disaggregating the different kinds of conflict. This essay focus on the use of the internet or cyberspace for armed conflict, review the utility and use of cyberattack, and considers the behavior of states, their military forces or proxies, and other armed groups in waging cyber war.

Questions persist as to the appropriate framework for considering this new mode of conflict, but to a degree these questions result from weak data, imprecise terminology and a certain reluctance to abandon the notion that cyber conflict is unique and sui generis, rather than being just another new technology applied to warfare. Imprecision in terminology hampers serious discussion of these issues. It is not correct to call every bad thing that happens on the internet "war" or "attack." The thresholds for war or attack should not be very different in cyberspace than they are for physical activity. We can also focus discussion by defining cyber war as the use of force to cause damage, destruction or casualties for political effect by states or political groups. A cyber attack would be an individual act intended to cause damage, destruction, or casualties. There is a gray area, of course, when we think about disruption, particularly the disruption of services and data, and when this disruption rises to the level of the use of force. The threshold should be very high for calling a disruptive activity an act of war or attack.

An act of war involves the use of force for political purposes by or against a state. Force involves violence or intimidation (the threatened of the use of force). These are useful thresholds for deciding when an event in cyberspace is an act of war or justifies the use of force. If there is no violence, it is not an attack. If there is no threat of violence, it is not the use of force. In making this distinction, it is important to note the role of clandestine or covert activities. If an opponent intends for a cyber exploit to be undetected, and if the exploit does not inflict physical damage or destruction, it is not intimidation, not the use of force, and not an attack.

We can also benefit from putting cyber war in the context of changes in military technologies and the resultant developments in strategy and doctrine. The weapons and tactics used by the Duke of Wellington not markedly different from those used by the Duke of Marlborough in 1700 a century earlier. One noted military historian goes as far as saying that Wellington's weapons and tactics were not that different from those used by Alexander the Great.[1] Technological change, the product of industrialization, mass production and the expansion of science transformed warfare. By the end of the First World War, the ability to create new technologies and exploit them for military benefit had become an essential part of conflict.

We can regard the internet as the latest development in a century of military innovation. The

[1] John Keegan, the Face of Battle, 1976

expansion of command and control and the reduction of uncertainty, part of the Clausewitzian "fog of war," changes how wars are fought. We know from experience that a networked force is more effective than non-networked for of similar size. Networked air defense is appreciably more effective than an aggregation of individual units. Armored vehicles, aircraft, and ships connected by data links will fight more effectively than their counterparts who relay solely on voice. This increase in effectiveness makes military networks a legitimate and valuable target for attack.

The use of network technologies and the exploitation of cyberspace for intelligence and attack has become a normal part of military activity. Cyber warfare will involve disruption of crucial network services and data, damage to critical infrastructure, and the creation of uncertainty and doubt among opposing commanders and political leaders. Cyber attack provides an ability to strike both tactical and strategic targets from a distance using inexpensive systems. Cyber attacks are unlikely to be decisive and will not by themselves produce victory, particularly against a large and powerful opponent. But they do offer strategic advantage and will be part of future military conflict.

We can now go beyond the disruption of networks and information to ascribe a kinetic effect to cyber weapons – the ability to inflict physical damage through cyber attack. The best evidence for this remains the Aurora tests at the Idaho National Labs, where a remotely transmitted command caused a major electric generator to self-destruct. There are other examples where accidental programming errors produced physical damage, suggesting that cyber attack can be seen as another long-range strike weapon – faster than missiles or aircraft, not as destructive, but cheaper and possibly covert.

For these reasons, all major militaries have or are developing cyber attack capabilities. The most significant "cyber-powers" have attack capabilities, have tested them, and plan for their use. The reconnaissance necessary to support them is routinely carried out. Cyber attack will form part of warfare in the future. One immediate issue is the applicability of existing laws of armed conflict to cyber attack. However, cyber attacks could have "strategic" or "tactical" application, depending on their target, with differing political implications for response, escalation, and international opinion.

To understand the role of cyber attack in war, we must ask of it the same questions we would ask of any other weapons system: range, destructiveness, cost, effect, and the political implications of use. Cyber attack has both tactical and strategic applications. It can be used against deployed forces or against strategic targets in the opponent's homeland (e.g. those that contribute to an opponent's ability to wage war. Its range is practically unlimited, in that it can be used anywhere the global network extends. It has a variety of delivery options, over networks, from dedicated platforms (ground, sea, air, space). While the preparation is for a cyber attack may be lengthy, the speed of the actual attack is measured in seconds irrespective of the distance from the target. The cost of an attack is low, and surprise and stealth are normal attributes.

There are disadvantages, however. We do not yet have the ability to scope collateral damage for all cyber attacks, particularly as a target set moves from tactical (such as deployed military forces) to strategic (such as civilian infrastructure). For attacks that disable networks, there

could be unpredictable damage not only to the target, but also to noncombatants, neutrals or even the attacker, depending upon the interconnections of the target network or machine. This makes the political risk of unintended consequences unpredictable (an attack on a Serbian network, for example, damages NATO allies' commercial activities) and carries with it the risk of escalating a conflict (an attack on North Korea damages services in China).

Cyber attacks are not very destructive, compared to other weapons, particularly strategic weapons. It seems fair to say that at this time, the possibility of damage, death and destruction from cyber attack is low. Cyber weapons will have difficulty productions casualties. An attack that caused a generator to self-destruct would do physical damage and might cause some casualties, but in general, these would be limited. For example, a turbine in a Russian dam that inadvertently self-destructed hurt electrical production, led to flooding, and resulted in ten or twenty causalities. This was a major accident, but we do not want to inflate its military effect. Cyber attack, in its physical consequence, is more like sabotage carried out by guerrillas or Special Forces. The weapon is, for all practical purposes, intangible, tiny electrical pulses whose lethality comes not form their own innate destructive capacity from the ability to instruct other tangible systems to malfunction.

Critical infrastructure is a normal target for military planners, to gain tactical or strategic advantage. Warsaw Pact planning for an assault on Western Europe targeted (among other things) power grids, telecommunications services, transportation hubs, fuel pipelines and government centers. Disabling these targets would have contributed to the speed and success of the ground assault. Cyberattacks could potentially provide the same disruptions (and possibly at lesser cost to any later occupation force). This is different from strategic attacks against manufacturing or other critical infrastructure where the intent is not to gain immediate tactical advantage, but to benefit from the degradation the opponent's capacity for sustained resistance. In this erosion of capability to resist, the utility of cyber attack is open to question, but the ability to interfere with communications and logistics for tactical advantage is not. For certain kinds of conflict, an opponent could reasonably be expected to use cyber attacks to interfere with efforts to move and supply forces.

Attacks on hospitals could produce casualties, by manipulating data, changing prescriptions or turning off life-support or other critical systems. While terrorists may find these kinds of attacks attractive, such attacks would be contrary to the existing laws of war. Harming noncombatants is unlikely produce much military advantage, but an opponent still might strike them (the same way that ambulances and hospital ships end up as "inadvertent" targets). Attacks on critical infrastructure, such as the power grid, might also harm medical services and produce casualties, but would not be considered contrary to the laws of war if there had been some consideration as to whether the value of the target outweighed the risk of noncombatant causalities.

In this area – the political consequences of cyber attack – the similarity to nuclear weapons may be greatest. Strikes on deployed forces, apart from their military benefits, will create unease and concern over potential escalation. In contrast, striking civilian targets, including critical infrastructure, in an opponent's homeland is a major escalation of conflict. The reaction of opponent leadership to attacks on civilian target in their homeland could be pronounced. An attack may be intended to be limited, but the opponent may not perceive (or believe) the

limitations. The uncertainty about the scope of collateral damage (and perhaps in attributing the attack) creates political risk from a decision to use cyber attack. Unexpected collateral damage may weaken international support, produce a negative domestic reaction, and stiffen resistance in target country. In this sense, cyber attack is a tactical weapon with strategic consequences.

One way to assess the utility of cyber "weapons" is to ask if any nation believes it gains coercive advantage from their possession or from their independent use. One concern held by both the US and the Soviets during the Cold War was that allowing the other side to gain nuclear superiority would encourage the opponent to engage in coercive behavior and, possibly, increase the likelihood of a surprise first strike. Cyber superiority only bears a small resemblance to nuclear superiority, which threatened a disarming and disabling first strike. A cyber first strike is conceivable, as part of a larger campaign, but a cyber-alone strike would serve only to warn and irritate an opponent. Cyber "weapons" or forces do not, in this sense, carry the same heft as conventional or strategic forces. An opponent could threaten cyber attack as a coercive measure, but the credibility of the threat would diminish rapidly if it was not carried out and if the target took defensive measures. Given their limited capacity for damage, cyber attack may depend more on speed and surprise to achieve an optimal effect.

Cyber attack introduces a new dimension, however, in the ability to create uncertainty in the mind of an opposing commander. Uncertainty forms a large part of Clausewitz's fog of war. Uncertainty slows decision-making, amplifies caution and timidity, and increases the chance of error. Misleading an opposing commander has always been part of warfare. Cyber attack provides a new and more intimate capacity to undertake this. Cyber attack potentially offer significant advantage in creating deception and undermining confidence. For example, the Allies went to significant lengths to deceive the Germans as to where they would land, by creating dummy armies and planting false information. The Germans may at first have hesitated to commit armored reserves again the Normandy landings, as they were unsure these were not a feint. The same kind of indecision could be produced by manipulation of data in a cyber attack. Beyond scrambling data, to deny an opponent access to it, a more damage (but also more difficult) maneuver would be to manipulate data, to make it incorrect

ULTRA, the British program to compromise encrypted radio communications that the Germans believed were secure, is a classic signals intelligence coup. There were sizeable benefits and the Germans did not suspect that they were penetrated. The same could easily happen today using cyber techniques. This is espionage, however, rather than an attack. Advanced militaries today are afforded much greater capabilities by cyber attack. Cyber attack provides a greater capability to interfere with command and control, since it provides an opponent not only intelligence but also the capability to disrupt. A cyber exploit that surreptitiously manipulated data in ways unfavorable to the opposing commander – something the ULTRA program could not do - provides a new dimension for cyber conflict. Additionally, an opponent could let their cyber efforts be discovered, to create distrust and hesitancy. The Iraqis were hampered by a fear that using their communications networks during Desert Storm would expose them to American signals intelligence. This slowed and complicated their decision-making.

If press reports are accurate, the Israeli air strike attack on the alleged Syrian nuclear facility illustrates this kind of manipulation. The strike was reportedly accompanied by cyber attack;

where the Israelis, perhaps using a mobile platform, were able to make Syrian defense radars show the situation as normal. Instead of a noisy jamming attack that would have alerted the Syrians, air defense radar screens showed the airspace as empty and peaceful, preserving the element of surprise. An astute attacker will use cyber techniques not only to better understand the opponent, but also to degrade their warning and response.

Cyber intrusions can degrade morale and the will to resist. Estonian and Georgian political leaders felt pressed by Russian cyber intrusions, although in the case of Estonia, the intrusions probably did more to increase resistance than to degrade it. During the second Gulf war, American forces sent Iraqi commanders emails urging them not to resist and providing instructions on how to surrender. This affected Iraqi resistance. A well-designed program, perhaps using spoofed messages on social networks, could become a source of damaging "rumint." During the Cold war, perhaps as a prank, East German reservists received a message ordering them all to report in uniform and assemble one Saturday. The bogus order created confusion and annoyance, and perhaps some intelligence benefit. It is not hard to imagine some kinds of cyber attacks interfering with logistics chains, rerouting supplies or making it appear that there are shortages or surpluses when the opposite is the case.

Each of these incidents illustrates how cyber attack can increase military advantage, but the capabilities provided by cyber attack will not be decisive, in the sense that a strategic weapon or a main force convention attack can be decisive. Instead, they will contribute to friction that slows, distracts, and perhaps weakens an opponent's response. French Resistance attacks on transportation systems during the battle of Normandy are an example of this. They were not, by themselves, sufficient to produce victory but they did provide a degree of advantage at little cost to the allied forces. Similarly, cyber attacks will degrade opponent effectiveness by some degree that will provide advantage but not by themselves assure an opponent's defeat.

The amount of advantage provided by cyber attack will depend in part on the scope and length of the conflict. Cyber attack will be more valuable in short conflicts. In conflict limited in time and scope, the disruption created by cyber attacks in services and logistics may provide an initial advantage, but then decline in utility as an opponent adjusts. In contrast, attacks against command and control, such as those that disrupt data and undermine confidence, in contrast, could have a sustained, cumulative effect and increasingly hamper an opponent's ability to resist.

This calculus could change if cyber attacks were able to damage industrial 'chokepoints," specific targets that would hamstring the ability to supply forces. The theory is sound, but particularly for large industrialized countries, it is easy to overestimate the ability to identify the full range of such targets, attack them effectively, and prevent an opponent from compensating for losses. The cyber equivalent of the 1943 Schweinfurt ball bearing raids,[2] which used air strikes in an unsuccessful attempt to cripple the production of new weapons by targeting an industrial chokepoint, would at least not be accompanied by heavy losses, but would likely be no

[2] As part of its larger doctrine of "strategic bombing," which used long distance attacks to degrade opponent production, transportation and morale, U.S. strategists identified ball bearings as a key component for weapons and machinery and decided that if the flow of ball bearings could be interrupted, German military production would be several damaged. The ability of the Germans to repair or to find substitutes greatly reduced the consequences of strategic bombing.

more effective in degrading industrial performance to a level that provided military benefit.

Attacks on infrastructure will have only a minimal effect in short clashes of only a few months, "go-with-what-you've-got" wars. The target nation's industrial capacity and the production of new weapons will be less important in these wars. We will not be fighting industrial-era wars of attrition between large regular forces and lasting for years. An opponent could successfully disrupt critical infrastructure, and if the target nation's leadership was able to manage the political implications of this, see little or no effect on opponent military capacity. It takes time for a disruption of industrial capacity to translate into a degradation of effectiveness in fielded forces. Attacks must be cumulative and persistent, to overcome opponent resilience and response. A short war could be over before cyber attack on critical infrastructure provided significant advantage.

The effect of attacks on infrastructure is easy to overestimate. Cyber attacks will resemble those actions where guerrillas plow up substations or pull down power pylons to remind the opposing government that they are there and to erode its legitimacy. Guerrillas do not expect to win as a result of these attacks. With the right leadership, large industrial nations are able to absorb many blows before there is significant damage to their ability to wage war. In some conflicts, in fact, there is a reluctance to do too much damage to infrastructure on the grounds that the attacking force itself will soon rely on it. In state versus state conflict, the issues for attacks on infrastructure in a peer/near-peer are if the military benefit of disabling infrastructure for some periods are outweighed by the risk of escalation, and in a large state/small state conflict whether the damage will harm any "nation-building' required in a post conflict situation.

We need to consider different scenarios for cyber attack to assess their probability and effect. Currently, the most probable scenario is a limited conflict between the U.S. and Russia or the U.S. and China, where our opponents would disrupt command and control, logistics and other services for theater forces. Opponents could disrupt rear services – bases external to the conflict zone including in the U.S., but they may be reluctant to move from military targets. Opponents would probably avoid strikes on critical infrastructure in the US homeland because of the risk of escalation, unless they were in extremis, in which case the risk of attack in the U.S. might be outweighed by some other factor (popular discontent with China's leadership, over the conduct of the war, for example). A move from the "tactical" application of cyber attacks to "strategic application holds political risk in that it could be interpreted as an escalation of conflict, justifying some escalated response, or it could affect international political opinion in ways unfavorable to the attacker.

Eventually, when regional powers like Iran or North Korea acquire cyber attack capabilities, and this may not be as far off as we assume, a strike against civilian targets in the US homeland will be more likely. Cyber capabilities will give these nations a strategic response. As U.S. forces struck targets in their countries, they would feel little or not constraint against attacking targets in ours. Both Iran and North Korea have not hesitated to use kinetic weapons and our assumptions about deterrence may not make any sense. Their calculus for deciding upon an attack is based on a different perception of risks and rewards. This alone makes a Cold War, one-size-fits all deterrent strategy of dubious value (what deters China may not deter Iran). The increased potential for cyber attack as small countries acquire the capability to strike distant targets is also

true for non-state opponents, and in a world of inadequate cyber defenses, disruptions for political purposes and even cyber attacks intended to damage or destroy could become routine.

Two interesting scenarios involve small (or smaller) states and insurgents. The first is whether a small state being attacked by a large state would perceive any political constraint from launching cyber strikes against the attacking power, particularly if the attack posed an existential threat. The second is whether insurgent groups will be constrained once they acquire a long-range attack capability. The U.S. was able to attack Iraq with impunity. If the Iraqis had cyber weapons, would they have felt unconstrained in using them against the U.S. homeland? These would not have changed the outcome of the invasion but would have provided a degree of vengeance. Similarly, the Taliban in Afghanistan or the Shabab in Somalia must fight in their own territory with little chance of attacking the U.S. homeland.

When they eventually acquire (or hire) the capacity to launch effective cyber strikes, a capability that these groups or regional powers like Iran or North Korea have heretofore lacked, Cyber strikes against the American homeland will become much more likely. These strikes will be appealing to them as it creates the possibility to bring the war to the U.S. homeland. But such attacks are unlikely to produce tactical advantage in theater and their political effects are difficult to predict. A population under sustained cyber attack may push its leaders to end the conflict, but the result could also be an increase in the will to resist and to continue fighting. Both outcomes have been seen in the past and in anything, striking the homeland (the hallmark of strategic bombing) seems to produce greater resistance. Insurgents are unlikely to make this calculation, however, and will use cyber strikes when they gain the capability.

There are of course many considerations other than the simple acquisition of cyber attack capabilities that will shape the ability of small state or insurgents to use cyber attack. While the tools are cheap, cyber attack is expensive as it depends on reconnaissance of network targets to find vulnerabilities and this reconnaissance must be periodically refreshed as networks change, add new equipment or software, or are reconfigured. A small nation or insurgent group that is plugged into the cyber underworld may be able to access such information, or to hire mercenaries. The key elements of a cyber attack capabilities are preparation and a fast “refresh cycle” for targeting. The ability to design and manage a large-scale attack might still be beyond their capacity, but harassment attacks against specific targets – Washington D.C., for example - would be possible. It is also likely that as digital network applications and processing capabilities continue to expand, there may be commercial services and programs that can be adapted to provide small groups with the necessary reconnaissance and planning capabilities.

This cursory review of scenarios suggests that the existing laws for armed conflict developed for kinetic weapons can be applied to cyber attack. The principles of distinction, proportionality, and discriminate attack must be considered to the same extent for cyber weapons as they would be for any other form of attack. There are, however, areas of ambiguity, including violation of third party sovereignty, the use of cyber attacks by terrorists, and the amount and nature of damage from cyber attack that could be interpreted as an act of war.

Some operational requirements, such as the degree of prior assessment of collateral damage required to make an attack consistent with the law of war, are also unclear. Attackers are

supposed to consider whether attacks on civilian targets, such as infrastructure, are legitimate. This decision requires assessing if the attack is "demanded by the necessities of war," whether resultant disruption or destruction would produce meaningful military advantage, and whether incidental civilian casualties or damage civilian property would be in excess of that needed to obtain military advantage. Such decisions are of course, arbitrary and depend on judgment. Insurgents and terrorist are unlikely to be burdened by these concerns and experience shows that the longer a war continues the interpretation of acceptable civilian damage tend to become more flexible and encompassing. Western nations, which tend to have 9at least initially) a greater regard for the rule of law, may be more hampered int eh conduct of cyber operations by these principles, although all attackers must consider the effect of indiscriminate attacks on world opinion and on the eventual political settlement of conflict.

The most important ambiguity is the threshold for regarding a cyber incident as the use of force. The right to self-defense is triggered by the use of force. This makes the question of the threshold between an act that justifies the use of force in response (an act of war) and an act that does not central to the discussion of cyberwar. An act of war is the threat or use of force against the territorial integrity or political independence. This threshold is by no means precise and leaves considerable room for judgment. While there is some consensus based on international practice that certain actions, espionage, crime, propaganda, do not justify the use of force in response, other areas are not so clear. When does a cyber reconnaissance become an act of war? Reconnaissance by itself is usually not considered sufficient justification, but a reconnaissance that involves leaving behind could be interpreted as an act of war.

Violation of sovereignty is an imprecise guide for deciding what is an act of war in cyberspace. Hacker, spies and criminals routinely send packets across borders with malicious intent. These actions are violations of sovereignty, but individually, they do not qualify as acts of war. Inserting a spy, whether physically or digitally, would not generally be regarded as a use of force justifying a forceful response, unless the violation could be portrayed as an attempt at coercion of intimidation. It could be argued that massive and repeated violations of sovereignty by cyber intrusion could be interpreted as an act of war and justify the use of force in response, but it would be incumbent upon the target nation to first notify the attacker that further intrusion would be regarded as an act of war. The failure of any nation to make this notification or complaint in the face of the massive cyber intrusions over the last decade means that we have not taken the opportunity to create a threshold (and perhaps a constraint) in cyber conflict.

Ultimately, the decision as to whether something is an act of war is a political decision, particularly in cases that fall into the grey area between annoyance and actions that attempt to end the existence of the state. The 1968 Pueblo incident involves force, violence, damage, and the violation of international law and that sovereignty o the United states, but did not threat he existence of the US and was ultimately interpreted not be an act of war. Two hundred and fifty years early, in the War of Jenkins Ear, Britain began a war with Spain after the removal of a British merchant captain's ear by Spanish coast guards who were looting his ship. While Jenkins' suffering was no doubt acute, it did not compare to the harm inflicted on the Pueblo and her crew. The best we can hope to achieve is to say that a cyber attack that caused or intended to cause damage. Destruction or casualties justifies going to political leaders for a decision as to whether this is an act of war or justifies a forceful response.

Disruption of data and networks, which is a form of physical destruction (ones and zeros are erased or replaced), could be considered an act of war but we would need to consider the scale and sensitivity of the data that was damaged. The author of the hostile act may also affect the decision that something was an act of war. When a deranged English activist defaced unclassified Pentagon websites and damaged networks in protest against the Iraq war, this was considered a crime, not an act of war. If a state had been involved, the action would move closer the act of war threshold. If a proxy was involved, and if the state sponsorship of the proxy could be established, it would also move closer to crossing the act-of-force threshold.

This threshold question is important for decisions regarding collective defense. The exploits against Estonia, for example, did not trigger the formal commitment under NATO's Article 5,[3] where an "armed attack" against one is considered an "armed attack" against all. Article 5 and its emphasis on the use of force has shaped western attitudes towards warfare and defense for sixty years, and NATO nations will need to carefully consider how to extend its application into cyberspace. The attacks on Estonia were intended to intimidate and to punish, but not to create damage. Lowering the threshold to make Estonia-like incident the equivalent of the use of force could have some deterrent effect against state opponents, but it could also be destabilizing, as many non-state groups and even individuals could launch similar denial or service exploits (but nothing more damaging) and a forceful reaction by defenders, even against the right target, could result in overreaction and increased tension.

This brief review suggests that in considering cyber war or cyber attack, we can place these actions into the existing framework of conflict and regard cyber, whose effects must be assessed and whose consequences must be considered in the larger political framework. This consideration will resolve around two thresholds that will shape strategy and doctrine for cyber conflict: the threshold for considering a cyber event and act of war and the use of force and the threshold between the tactical and strategic application of cyber attacks. The analysis of when a cyber event crosses these thresholds will determine their use and the response to their use.

Digital networks are a new tool for state power. Cyberattack will be part of future military conflict. Like earlier technological innovations, they will be used and perhaps reshape warfare. Some of the issues and ambiguities identified int his paper will not be resolved, unfortunately, until we gain further direct experience in cyber warfare. In the interim, war games and exercises can provide insights. Dialogue with potential opponents and with allies can also begin to clarify issues and perhaps reduce the chance of miscalculation or misperception. Additional studies with greater methodological rigor than has been seen in the past could also help define cyber war and provide guidance on the use of cyber attacks, their risks, and potential responses.

---

[3] Article 5 of the North Atlantic Treaty states: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."