



EXECUTIVE DIRECTOR'S COMMENTARY

ASYMMETRIC WARFARE AS A TACTIC OF HYBRID WARFARE: CHALLENGES AND RESPONSE¹

PfPC Executive Director's Commentary No. 2 / Apr 22, 2016 / www.pfp-consortium.org

EXECUTIVE SUMMARY

Asymmetric warfare is that aspect of hybrid warfare in which individuals or small groups leverage weaponry or technology to inflict damage far out of proportion to what would have been possible for the same actors in a conventional war. Countries have two options: either overreact to incidents of asymmetric warfare, or else reach a steady state of resiliency where new cases – horrible as they may be – can be withstood by society.

No country – especially a democracy – can remain fully mobilized indefinitely. Our goal should be to manage asymmetric attacks without descending down the path of a police state, with the loss of freedom that such a path would entail. In dealing with asymmetric warfare, we must be prepared to acknowledge and accept the inevitability of asymmetric attacks and losses, while maintaining the resiliency of our society to function in their aftermath.

Before I begin, I would like to say a few words about the Diplomatic Academy. Those of you who are students here are fortunate indeed. The DA has superior academic programs and faculty to prepare you for future leadership positions. The world has a dire need for leaders with the skills you are learning, because too often the alternative to effective diplomacy is violent conflict.

Asymmetric warfare as a subset of hybrid warfare

This panel concerns asymmetric warfare. Clearly, war has changed over the centuries. The most recent incarnation is often called “hybrid warfare,” of which asymmetric warfare is a key component.

Hybrid warfare has many definitions, but for our purposes today let's take it to mean unrestricted warfare, using all possible means to accomplish political and military goals. There are no rules: no chivalry, no ethics, no Geneva Convention.

The instruments of hybrid war are numerous: propaganda, disinformation and subterfuge, conventional combat, sabotage, cyber attacks, economic warfare, guerrilla actions, insurgencies, asymmetric attacks by small groups with high-impact weapons, political negotiations or deceit—you name it. Within this context, one could also ask whether forcing or facilitating mass migration of refugees is a tactic of hybrid warfare as well.

¹ Remarks by Raphael Perl, Executive Director of the Partnership for Peace Consortium before the 12th Annual Student Conference: *Hackers, Contractors and Drones: Warfare in the 21st Century*, The Diplomatic Academy of Vienna, April 22, 2016. Please note that the viewpoints represented here are personal, so opinions expressed may not represent official positions.

So how does asymmetric warfare fit into the picture?

Asymmetric warfare – in a nutshell – is that aspect of hybrid warfare in which individuals or small groups leverage weaponry or technology to inflict damage far out of proportion to what would have been possible for the same actors in a conventional war.

Asymmetric warfare is when a seemingly harmless child is wearing a suicide vest and detonates it, causing mass casualties. It is a disgruntled political activist poisoning a coffee urn.

Whenever we talk about asymmetric warfare, we should keep in mind that it is a tactic delivering an effect, and not a cause. Trying to stop it is like treating the symptoms of a disease without addressing the underlying cause; it doesn't work. We can't protect everything, everywhere, all the time, and efforts by governments to do so will inevitably fail.

No country – especially a democracy – can remain fully mobilized indefinitely. The cost is too high, and the strain is too great. Sooner or later we relax and become complacent. In Paris in the 1980s there were terrorist bombings. Trash cans along the streets were welded shut. Airports had open trays for trash, so everything would be visible. Bands of soldiers with automatic weapons patrolled the airports and metro stations. A decade or so later, the trash cans had long since been reopened. The soldiers were in their barracks. Bombings began again, perhaps for unrelated reasons, at a time when the intensity of vigilance by the government had diminished.

At the height of the anthrax threats in the US, large areas were closed off every time someone found a package of white powder. Special post offices were set up to irradiate mail sent to public officials. The costs were enormous. It isn't at all clear what the benefits were in the long run.

Responding to asymmetric warfare

The bottom line is that countries have two options: either overreact to incidents of asymmetric warfare, or else reach a steady state of resiliency where new cases – horrible as they may be – can be withstood by society.

We should therefore adopt a policy of “acceptable losses.” Countries with ongoing violent internal conflicts end up rapidly adjusting to this approach because they have no choice. Whatever the reason for the conflict, life and commerce must go on with a semblance of normalcy, even in the midst of chaos.

So how does one go about accomplishing this? One hardens the important targets, buys insurance for the softer targets, encourages people to be alert, and accepts the fact that asymmetric attacks are going to happen. Any government that seriously tries to monitor every threat within its borders in real-time will end up as an oppressive autocracy, and still won't be successful at stopping asymmetric attacks.

The ultimate nightmare scenario of asymmetric warfare is the so-called “nuclear option,” which we should not dismiss and must prepare for. The same applies to chemical and biological weapons. This is a very unpleasant reality, but it is better to face it and plan now. We have seen chemical agents used from time to time both in active conflicts in the Middle East and in Japan and England. If weapons of mass destruction are available to countries or groups with violent goals – whether political or cultural – sooner or later they are likely to be used.

Some policy options

What can be done to defend against asymmetric warfare? I offer for consideration two major components: *intelligence and action*.

INTELLIGENCE

Analyze: Monitor and review world events as they unfold. Important here is monitoring social media and other communications networks to identify surge activity and trends, to include the use of state-of-the-art data correlation techniques for predictive purposes.

Detect: Identify unusual patterns of activity.

Validate: Confirm anomalous activity and relate to possible sources or origins of attacks. Network analysis is an important tool here.

Identify Actors: Establish chains of command and causality from sources to proxies to individuals.

Predict: Attempt to anticipate upcoming asymmetric attacks, maximizing data sharing among international law enforcement and border control agencies.

ACTION

Engage and Disrupt: Mobilize resources to neutralize the logistics and counter the motivation and ideology behind asymmetric attacks.

Pre-empt: Where appropriate, and where supported by overwhelming evidence, use first strike capabilities on various fronts to deter asymmetric attacks before they can be planned or carried out.

Mitigate: Make realistic, specific contingency plans for a wide variety of likely asymmetric attack scenarios.

Counterattack: Use a variety of tactics to neutralize opponents.

So far I have only addressed one side of the story here. Western countries are not only the victims of asymmetric attacks, but indeed employ this approach often. Through the leveraged use of surrogates, drones, and cyber attacks, it is possible for major state powers to participate in wars – whether declared or undeclared – without the enormous costs of “boots on the ground”.

However, history would suggest that it is difficult to implement durable cultural or political change in another country without putting boots on the ground and without huge expenditures and decades of presence and involvement, during which the education of youth targets new generations with the goal of changing their perspectives.

CONTACT INFORMATION

For more information, please contact:

Dr Raphael Perl, Executive Director

Partnership for Peace Consortium

Raphael.Perl@pfp-consortium.org

OR

The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Operations Staff:

pfpconsortium@marshallcenter.org;

www.pfp-consortium.org

So, if you ask is asymmetric warfare the wave of the future – in effect replacing conventional warfare – my answer is no. Conventional warfare will remain a viable military option for the foreseeable future.

In the future, the arena of international conflict will become much more complex, and the role of asymmetric warfare will become increasingly important.

Today, technology facilitates the rapid implementation of asymmetric approaches. Communication is instantaneous, and encryption can make it secure. International commerce has reached a scale at which the screening and tracking of contraband is far from 100%. Many borders are not secure. Times have changed.

This situation may sound like a state of perpetual warfare, and indeed it is. Peace is not the normal status quo for mankind. Some societies, cultures, religions, or other subgroups regard violent conflict as a noble cause, rather than something to be avoided.

Conclusion

In conclusion, I'd like to leave to you with the following thoughts: asymmetric attacks are here to stay. We should expect both conventional and unconventional conflicts in the future, and should ensure that the size and configuration of our military defenses – and our offensive actions, if necessary – are appropriate, proportionate, and affordable. Our goal should be to manage asymmetric attacks without descending down the path of a police state, with the loss of freedom that such a path would entail. In dealing with asymmetric warfare, we must be prepared to acknowledge and accept the inevitability of asymmetric attacks and losses, while maintaining the resiliency of our society to function in their aftermath.