Peter Zwack

OLD TACTICS, NEW TECHNOLOGY: HYBRID WARFARE'S NEW SCRIPT FOR THE WORLD'S ARMED FORCES

ABSTRACT: *Brigadier General (Ret.) Zwack sums up in his speech the very basics of hybrid warfare and the potential countermeasures.*

KEYWORDS: *hybrid warfare, definition of hybrid warfare, gray zone, role of technology, below-threshold capabilities*

ABOUT THE AUTHOR:
Dr. Peter Zwack is a retired Brigadier General of the U.S. Army

General, good to follow you in this discussion.

General Sándor, Colonel Bárány, my old friend Lieutenant-Colonel László Ujházy, and Dr. Péter Kiss who worked with me in the 66th Military Intelligence Brigade thirty years ago. What an honour it is for me to have been invited to speak to you today about a really serious topic that all of us would define in a different way, and that is one of the challenges. I feel among friends when I say that, allies, partners, and even countries where it has been difficult relationships in that way as well. The first time I was in Hungary in the military mode was, like, around 1993, and it just shows you how the world has changed: I was in the 3rd Infantry Division and we came down to watch a Hungarian infantry and engineer river crossing of the Danube River at Ercsi.

And how the world has changed! We watched Hungary's progression in becoming a NATO ally. I worked with a Hungarian guard battalion and teams in Kosovo, and in the world of hybrid and complexity even got out to Pol-e Khomri, to your PRT. So, there is a long history here and again a huge honour. I am sorry about this long preamble, but this is very special for me. I must say it is quite the honour to be asked as one of the early keynote speakers in this important and timely conference.

Therefore, I see my early role today as setting the proverbial table up with some broad thoughts and perspectives regarding hybrid warfare and its challenges for armed forces both independently and as operating as allies. I will emphasize that over and over again not just in traditional warfighting. But anyway, what is traditional warfighting anymore, I wonder. Does it really exist anymore? Especially when facing hybrid type threats that as much attack the mind and our functional and psychological nervous system as specific military systems and functions.

For me it is important not to get mired, bogged down, in the academic definitions of hybrid warfare that I feel put us in a cognitive box. We have all tried to pin it down while also parsing out other terms related to hybrid in nonlinear, new generation, new type war, irregular warfare, military operations other than war or MOOTW, irregular warfare, asymmetry and many more. But in this day of comprehensive connectivity through the depths of

societies and their militaries, what is the difference anymore between so called conventional and unconventional warfare?

Suffice to say, to me hybrid and the so called gray zone is a domain that lives between full war and full peace, one in which we live every day and we are in it now as well whether militarily or in our societies. When we discuss the definition for hybrid warfare, I prefer the analysis by Frank Hoffman, a friend of mine from the National Defence University and a professor. He writes that hybrid war is a tailored mix of conventional weapons, people, irregular tactics, terrorism, and criminal behaviour in the same battle space – all mixed together in the same battle space, to obtain political objectives.

I am going to do now something that is fairly basic, and perhaps not usual in a scientific conference, but I want to get to the very basics of hybrid war. I am not a high academic, but I want to talk to you about the vocabulary – just the fundamental vocabulary of hybrid warfare. I am going to go through a list of words just to reflect on the subject. You may find this purely elementary but I think that just to get our heads wrapped into how we grapple with this.

First of all, when we talk about hybrid, what are the **targets?** What are the objectives of hybrid? What is it that a nation or group is trying to do? The targets, I would say, from the top down are societal, political, alliances, and with that cohesion – the Clausewitzian centre of gravity works through all of that. Also, units of all sizes. How about individuals within those units with their smartphones?

Will – this is such a critical word. Will – whether at national, domestic, group or individual level. The will to fight, the belief in your system, the belief in your nation. All of that. And we saw a well-armed Afghan military collapse in August, I believe first and foremost because psychologically they lost their will, lost their belief.

And then again, I think **cohesion and centre of gravity,** which is where I believe a hybrid campaign is targeted at every level. And with all that there are tribes, clans, population groups, political parties – it is all of it.

Intent. I have talked about targets. What about the intent. These are timeless, I mean obvious words, but I refresh.

Surprise. Highly unconventional, right down on the ground, in everything that goes on within the world of hybrid. Usually in the hybrid world, the opponent is often overmatched by what we would call strength or power, but will gain a little, gain equivalency in surprise in other ways.

Disruption. A classic military word, but also applies to the populace.

Deception. We live through this in this world every day.

Paralysis. The inability to make a move and, as you know, a shock right through your system.

Confusion. A word in English I like to use is warmongering, creating fear and anxiety among target groups, amongst the people.

Division. Dividing societies, dividing through belief within the ranks.

Demoralization.

Distraction. Meaning when we are moving into a potential fight or whatever we need to be focused, and anything that distract us – a disease or anything else – makes us weaker.

Tactics. How about just simple things like false flags. We see that in the cyber world, especially today. Non-attribution, media insertion, insinuation, stealth tactics. All these are timeless in conception, but with a new technological backbone today.

Means and delivery. You know we talked about means and delivery in a military sense, firing things. But it also very much applies to hybrid. A whispering campaign as in the old days, you know, rumours and all of that. Media and social media – they are similar but different.

Cyber – viruses, phishing, stealing, all of that, which we are all very prone to.

Sanctions, economic, infection, all of these things.

And, frankly and most importantly, **imagination,** that is, anything that you can figure out in the hybrid world imaginatively, against what you perceive as conventional thinking, is potentially quite effective.

Role of artificial intelligence. China is leading the way on that. How does that play out here?

So, the result is that we have to deal with all that as targets, but also in our own offensive campaigns. Again, the intent is similar – disruption, confusion, distrust. Look at the distrust out there in the world of information and intelligence. Paralysis, miscalculation, hesitation, indecision, ridicule. Functions for the military that today in this cyber-fast world we have to make decisions clearly and quickly, and anything you can do to cloud that can change the mental correlation of forces and bring about division and then defeat.

Then finally, how to counter this. The good news is that NATO and in some of our NATO countries there are now centres of excellence in cyber and in hybrid warfare, they are beginning to work pulled together. It is inoculation. That is the word I would use – it is psychological, first and foremost.

Crosstalk, the criticality of cross talk.

Integrated fusion, meaning you have fusion centres and you are not working in stove pipes where you are vulnerable. Saying that, within those stovepipes you have redundancy, and you need redundancy within that fusion. It cannot all be in one place.

Civil-military fusion. We are struggling with that in the United States. The firewall between military and civilian is critical when you are living in the world of cyber and hybrid, where there are no boundaries and there is no rear zone. Everything is alert, quick reaction, moving fast, seeing it being able to process it.

You have to know your own **vulnerabilities.** It is one thing to focus on the potential adversary, we have to know our own vulnerabilities and then work within that system to adjust. How about honesty and an open society in your assessments. If you were all closed up and cramped, you know you cannot crosstalk the way you would want to. However, with it there is also a vulnerability, which is the open society, which of course the world of hybrid feeds on. And this is a challenge for democratic leading nations with open societies.

Finally, **deterrence.** How do you deter hybrid actors whether criminal or state owned and we grapple with that. And I go back to it again – imagination. It is fighting the failure of imagination. For example, 9/11 in the United States was a failure of imagination of our own side to see what was going on, although all the pieces were there. Afghanistan August, just now, was a failure of imagination. What could happen and what happened so fast and then for the Americans, talk about Pearl Harbour all the indicators were there and a lot of them were out there out in the hybrid world and we just missed it.

In the United States, I just throw out a couple of magazines here, because people are focusing on this new age. In Newsweek, Risk of a New Cyber Pearl Harbour. What it is doing is opening thoughts. In Harper's, just now, The Coming Battle in Space. Space also can and will be, if we ever get to do something really combative there, a hybrid domain, because it has an enormous effect on everything that goes on on the ground.

Threats today can come from any direction, at any speed, especially against ill-prepared entities, against which the armed forces can be ineffective. We have all read accounts of the various ways Ukrainian forces were hit in the Donbass, whether by cyber, electronic warfare, PMCs, media disinformation, proxies, assassinations, and much more. Those forces involved in contact, and also to those way back deep in sanctuary. We grappled with that in Iraq and Afghanistan as well.

Does this sanctuary work anymore if an individual or unit is switched on? What I mean by "switched on" is that as soon as you have turned on your smartphones or your systems even in a so called sanctuary, you are now plugged into the world of hybrid and need to be protected. The famous term is "strategic corporal."

In that realm, I am reminded of two well-known societal and/or strategic hybrid instances. Many among you know better than I do that Estonia was brought to a standstill in 2007 due to unattributed cyber-attacks linked to the Soviet bronze statue incident. In 2017, during the onset of NATO's Enhanced Forward Presence battalion deployments in the Baltics, disinformation was put out, falsely insinuating that a Bundeswehr soldier raped a local child. Initially it shocked the public, but the good news is that the disinformation was quickly defused by a coordinated Lithuanian, German, and NATO reaction. So, bad news, but then good news on that. And this is the tip of the iceberg when we consider external national level hybrid efforts in both Europe and in my country, as noted by our 2016 and 2020 election hacks and interferences. The aim was to subvert governance and confidence in the democratic processes influencing media platforms and corrupting political parties all of which affect the morale, cohesion and focus of our armed forces, and I submit that we all grapple with this.

Then on a macro scale: in May 2021 – and you all read about this, it was a big deal – ransomware hackers, likely a Russia-based dark side criminal group, shut down the over five thousand miles gas pipeline, disrupting much of the power grid in the eastern United States. This went on for quite some time. The effect was quickly resolved by an unpopular four million-dollar ransom payment. The episode highlighted the world's growing vulnerability to destructive attacks by unconventional players using sophisticated technology and techniques, but at the same token cheap, inexpensive, and anybody with the smarts can figure it out.

Whether it was a criminal or a state sponsored organization, there can be no doubt that the effects were strategic in nature, and risked a strategic response matching the scale of the attack, especially if, God forbid, innocent people had been killed.

If that thing had occurred in winter, while other things were also occurring, and our defence system is surprised – we do not know what is happening, where it is coming from – then our readiness level goes up it starts to get really militarily dangerous. Could you imagine if a giant river dam or valves in a chemical complex are stealthily cyber-opened from afar? It could be a criminal, but how it brings in defence involved now. Or how about nuclear command and control. It all sounds very military, but it is very hybrid, a whole-of-society vulnerability.

Non-attributed private military companies, PMCs, such as the Wagner group and local proxies, carry out aspects of foreign policy with little accountability and deniable visibility. Particularly alarming is the fact that today's hybrid warfare methods are faster, easier to obscure, and potentially far more lethal. As our societies and economies become increasingly knitted together around the world, we can no longer depend on borders or geographic distance to supply defences against bad actors.

Warfare is not limited anymore to physical battlefields or conventional or just conventional weaponry, the Internet, global finance, supply chain and other interconnected systems are subject 24/7 to manipulation and misuse designed to destabilize populations and societies. A catastrophe in one country can easily have ripple effects within the greater region or region around the world.

How does this new state warfare effect our militaries? I have already touched on this, the impact is profound. Not only are individual soldiers in units subject to the influence of disinformation and other disruptive campaigns, but our militaries as a whole must be prepared to expand their below-threshold skill sets beyond conventional ground and air warfare. This is already happening and the fact that you are hosting this conference is a real good indicator that you know our minds are in it. But how we get to thinking and down into action in the units is also a major task.

Another example, cheap drones, that just one of many examples first created for peaceful applications now are potentially game changing weapons especially when unleashed in large numbers such as we saw in Armenia and Azerbaijan last summer. With tensions increasing between Russia and Ukraine and greater NATO-EU, the ongoing major disruption caused by Belarus surging and hybrid-weaponizing migrants into NATO territory, Poland and Lithuania, in the general territory of the sensitive Suwalki gap, separating core Russia and Russian Kaliningrad, further destabilizes European security.

As electronic weapons and systems eclipse older technologies, the ability to recognize and analyse incoming threats quickly and accurately will become more important than ever. It is no exaggeration to say that the difference between being a peacetime and wartime commander now it is just a matter of flicking a switch – really cognitive. While below threshold gray zone activities are switching on and off a switch.

Russian chief of the general staff Valery Gerasimov just recently noted he said it several times that the lines are increasingly blurred between conventional and nuclear war and by inference this is the gray zone. With hackers and other bad actors targeting the established systems we depend on communication, so there is the ever-present danger of deadly misunderstandings based on false information. So how should our armed forces address this ongoing threat to our societies and our military organizations during “peacetime”?

Swift awareness is the number one priority. The ability to recognize false damage and misinformation quickly is critical. Second, and I cannot emphasize this enough, second, crosstalk between all echelons up, down, and laterally is essential, which has significantly improved within NATO and EU. This is especially important for the vulnerability for the vulnerable permeable wall between military and civilian entities. Third, military interoperability on which we all grew up with in NATO, and the Partnership for Peace is bigger than that now. Between allies and partners must be closely coordinated not just in system capabilities and tactics, techniques and procedures, TTP, but also in the psychological and material aspects of hybrid warfare across the full spectrum of peace and war and the below-threshold, enormous gray zone in between.

While the short discussion focused on European and western security I would be remiss not to mention that hybrid warfare activities have been along and played in other non-European nations and global regions the Middle East, whether Israel or Hezbollah, Syria, Iraq, Yemen. Afghanistan, Africa and South American bubbles and the China aspect of this is daunting as we see now increasingly the Chinese concept of unrestricted warfare playing out.

In conclusion, no nation today can successfully ignore or cope on its own with the threat presented by hybrid warfare and the ever expanding gray zone between peace and war. A hybrid war can be local and tactical or by leveraging disinformation, economic coercion such as pipeline brinksmanship, and political subversion, it can encompass higher regions, nations and continents.

The world's best hope for engaging in a successful fight against the many-headed hydra that constitutes hybrid warfare will require unprecedented and unceasing coordination and good faith, cooperation between trusted allies and partners locally and globally. In doing so, they must collectively and convincingly ensure that the deterrent costs for such malign actions and behaviour are prohibitively high for those nations and entities that engage in them.

The fundamental objective of hybrid warfare is as old as time itself. The fundamental vocabulary of intent and desired result, which I just touched on briefly, as well as the whispering campaigns seeding disorder and dissent are much the same today as they were a thousand years ago. The blink of an eye delivery systems however are an RMA, a revolution in military affairs and mandate that we all remain ceaselessly vigilant and coordinated.

I brought a copy of a book with me that I'm going to bring tomorrow and give the director of this great program. It is *Hybrid Warfare, Fighting Complex Opponents from the Ancient World to the Present,* and it goes back to what I discussed here, old tactics and new technology. It was written number of years ago by a friend of mine on the Joint Staff, Peter Mansoor. It is superb. It gets into a dozen campaigns around the world, going back to the Teuronburg Wald and the Romans a thousand years ago, about how hybrid will work in some of those things. To close, I am honoured to have been invited and I look forward to be with you the next couple of days.