Terrorism – Studies, Analyses, Prevention, 2024, no. 5: 423–434

https://doi.org/10.4467/27204383TER.24.016.19404

I believe we can handle the new threats!

Interview with Col. (Ret.) Christopher P. Costa, former counterterrorism advisor to the US president and director of the International Spy Museum in Washington, DC

The world is changing at a rapid pace. The nature of modern threats is also changing. The unstable geopolitical situation, the rapid development of new technologies, the emergence of cryptocurrencies and artificial intelligence are causing security services to face new challenges. How can they prepare for them to more effectively counter emerging threats? Colonel (Ret.) **Christopher P. Costa**, a long-time US intelligence officer, answers this question by referring both to his own extensive experience and to the history of global espionage and terrorism. He points out both the need to critically analyze the lessons of the past and the services' ability to take advantage of new technological opportunities. He stresses the importance of exchanging information and developing cooperation at the international level, and emphasizes the role that public education plays in prevention efforts. He sees the promotion of knowledge as the mission of the International Spy Museum in Washington, which he directs. The interview was conducted during Director Costa's visit to Poland, and the conversation is accompanied by reflections on the current situation in Central and Eastern Europe.

Damian Szlachter: The interview will be published on the 20th anniversary of the attacks on Madrid's commuter transport system, widely accepted as a European awakening in the fight against terrorism. However, I would like to start this conversation with another event, a symbol of the end of the 20th century. If I may ask, where were you on September 11, 2001, where did you find information about the attacks on the WTC and the Pentagon, and what were the immediate consequences for you?

Christopher P. Costa: When 9-11 happened, I had just moved to New York State, which is located just up the river from New York City in Albany. At the time, I was taking command of a recruiting battalion, a role that involves overseeing the enlistment of young individuals into the Army. Before this, I had spent my career as an intelligence officer in combat zones even prior to 9-11. However, the Army decided to assign me to a recruiting battalion, which was not where I wanted to be when the terrorist attacks occurred.

Initially, I felt bad that I wasn't with my colleagues who were fighting in Afghanistan. I had to spend the next two years learning about the Army and its mission. However, I decided to use this opportunity to study terrorism. I taught a class on terrorism in the evenings while also managing my other responsibilities. I spent a year and a half studying terrorism, almost obsessively, to understand this dynamic better.

Although I wasn't overseas, I kept waiting for the call to deploy. I wanted to use my skills and knowledge to help in the fight against terrorism. Eventually, before I changed command, a general officer called me and asked for my help with human intelligence in Afghanistan. I eagerly accepted the opportunity without hesitation.

When 9-11 occurred, I was in New York State, and just like most everyone else in the world, I was appalled by it. However, I also felt a little sorry for myself at the time because I wasn't in a position to use my skills and training overseas. Looking back, I realized that this experience was positive for my personal development since it allowed me to take the time to study and prepare for the counterterrorism fight. Thank you for that question.

When reading your biography, you can proudly say that you have worked in every area of the US counterterrorism system, from operational work, through the tactical level, to the strategic level, headed by the President of the United States. In each of them, the coordination of many entities participating in anti-terrorist activities is extremely important. My question is how to maintain a high degree of coordination at each of the three levels, what is your personal experience with this?

Ch. C.: Just how to coordinate all those entities on the operational, tactical, and strategic levels is more art than science. So that's an important question. And I will tell you that although I worked at the operational and tactical levels, on multiple deployments for many years, when 9-11 happened, I had not, as of yet, served at a strategic level. I have always served in operational and tactical levels. I had certainly been conducting operations that I knew the chairman of the Joint Chiefs staff, for example, would have visibility on to brief the President on if required, but I had never seen the complete strategic-operational-tactical cycle until I had the benefit of serving at the White House. And on the point of the White House, please allow me to digress for a second. I love that you produce a journal such as this ABW journal, because I'm a lifelong learner. And I've already suggested to you that my studying terrorism and teaching in the aftermath of 9-11 helped me get my head around these problems. I had read about national security decision-making. I was fascinated by how powerful government figures make decisions, and how leaders on a battlefield make decisions. So, when I had the opportunity to go to the White House, and I had the opportunity also to see how we worked together with foreign partners, and how we built a counterterrorism enterprise to focus on a global fight on counterterrorism, those experiences came together for me when I served on the National Security Council at the White House. And that's when I was the convening authority for the interagency, meaning I was roughly a three-star general officer equivalent, assistant secretary level in our system. There, I was able to pull together the interagency to focus on strategic threats. And the secret to my success, if I had success at all, was having the humility to know that I didn't have all the answers, having the humility and experience to know that I have to represent and let others offer their opposing views. I knew not to 'fall in love' with my recommendations on policy and

courses of action for the President to decide on. I learned all of that on the battlefield. So those experiences helped me serve at the White House. But I never saw the strategic, operational, and tactical come together until I served at the National Security Council. And what a tremendous experience that was.

The 2018 National Strategy for Counterterrorism of the USA is a pillar of the US counterterrorism system. At that time, Poland had a National Anti-Terrorist Programme which performed a similar function. How to effectively supervise the implementation of such a strategy by state authorities? In other words, how to assess the timeliness and quality of implementation of strategy tasks by area leaders and their supporting institutions? How was it solved in the US?

Ch. C.: We began shaping the 2018 National Counterterrorism Strategy the day I came into the White House by operationalizing counterterrorism ideas. And frankly, most of our efforts were focused on kinetically going after terrorists in places like Afghanistan, and on the ground in Syria and Iraq. So while we were implementing strategies, while we were accelerating our approach, we were also framing what our strategy looks like. There was a time that I believed our strategy should almost singularly focus on the jihadi threat because we were so focused on Islamist terrorism. But then my team concluded that there are other threats, too, and built in the far-right threat, and other extremist threats to include, in the 2018 strategy, you'll see the word Nazi used or the organization Nazis used because we recognized that we had to go beyond the jihadi threat. So the wisdom of the interagency coming together with a feedback loop, hearing from all of the agencies responsible for terrorism, we recognized that we needed to build in words and framing on domestic violent extremism, on counter-radicalization, on the far right, and any kind of extremism that could lead to political violence. So for the first time in the nation's history from a policy standpoint, the United States talked about domestic terrorism. And remember, we had our terrorism domestically in Oklahoma City in 1995, but we had the wisdom in 2017-18 to recognize a changing terrorism landscape. Despite the focus on ISIS, Al-Qaeda, Afghanistan, Iraq, and Syria, we knew that we needed to focus on domestic terrorism,

too. That said, it's now 2023 (the interview was conducted in August 2023 - editor's note), and there's been an evolution of thinking on terrorism threats, and the current Biden administration did what I think is right, and that is to say, they focused a strategy on domestic violent extremism, and they published that soon after the new administration came on board.

Indeed, the threat evolves. I didn't expect the 2018 strategy to last forever, but I'm really happy that it lasted until this year because that represents a solid strategy that helped the last administration and the current administration. And just one other focus on how do you assess implementation? So that is the mechanics of, as we say, sausage making. The interagency is responsible for identifying specific measures of effectiveness and performance, and they go back to the National Security Council and find out how many attacks were disrupted, and how many intelligence agreements with partners across the world were impacted, for example. The interagency takes those lofty words in a strategy and turns them into measurable and implementation instructions because it's easy to write an overarching strategy, but the challenge is implementation and measuring performance and success. What's much more challenging is implementing that strategy and assessing the implementation of that strategy.

Currently, on the eastern flank of NATO, we have an unprecedented situation related to the internal security of countries bordering the Russian Federation and Belarus. In the opinion of national and EU experts, in the next three years, terrorist activities should be expected to be used for hybrid activities carried out with the support of state entities. These activities will focus on attacks disrupting the continuity of operation of critical infrastructure (e.g. transport, energy, telecommunications). How to work on increasing the resilience of such facilities strategically for state security?

Ch. C.: Currently, in our eastern flank of the NATO, we have an unprecedented situation related of course to the internal security of countries bordering Russia and Belarus. According to national EU experts, in the next few years, this activity should be expected to be used by private activities carried out with the support of those

states. Those activities will focus on attacks disrupting the continuity of operational or critical infrastructure, of course. How to work on increasing the resilience of such facilities as critical infrastructure? So this gets to the heart of what I think the challenges are. I think Putin is going to become increasingly unhappy with his ability to wage conventional warfare. So he is going to revert more deliberately to infrastructure attacks. As such, the heart of your question is really important. And we know Russia has a history of, as somebody from the Internal Security Agency (ABW) has pointed out, of maskirovka, and not only disruption but disinformation, subversion, covert actions, assassinations, all things we talk about at the Spy Museum from the lens of history. But those activities are going to begin to happen outside of Ukraine to increasingly put stress on the alliance of NATO and other partnerships. So critical infrastructure, not only from a cyber-standpoint but also physical infrastructure is crucial because it's vulnerable to sabotage. We've seen dams that have been disrupted. We've seen bridges that have gone down in Ukraine, railways, and other infrastructure at risk. Again, from a special operations standpoint, we know history is a great guide to the way nations have handled special operations and counter-subversion. As such, I think the importance of the ABW, the importance of lessons learned, and sharing those lessons learned, are crucial. And I've said this elsewhere, this isn't just for you. I say this to my friends at the FBI, and to generals at Special Operations Command, the 'coin of the realm', so to speak, is counterintelligence going forward, because the threats are going to be hybridized, meaning intelligence services are going to behave increasingly more like terrorists. We see that from Iran in their employment of proxies. We see that in Russia. Proxies are going to be mobilized to do more increasingly lethal and dangerous things. I think, then, that the heart of your question is important, but I also have faith in the Polish security services, and you're asking all the right questions. I do. I read Polish history. I'm very impressed by it. I mean, I've always been a fan of Polish military and security capabilities. Unfortunately, as you all know, historically, Soviet-German disinformation in past years has tried to propagandize a false narrative about your impressive nation. We know that Poland has been a strong military power throughout history, but you have also fallen victim to some of your geography.

Photo: Christopher P. Costa, Director of the International Spy Museum in Washington (left), and Damian Szlachter, Editor-in-Chief of the magazine "Terrorism – Studies, Analyses, Prevention", during the meeting at the Central Training and Education Centre of the Internal Security Agency in Emów.

Source: own materials.

What are the challenges faced by Western secret services and law enforcement agencies that carry out tasks to combat terrorism in this decade of the 21st century? How to improve their structures, personal potential, or technical resources against terrorists using unmanned systems, 3D printing, cryptocurrency payments, and professionally encrypted instant messengers or hidden forums on gaming platforms?

Ch. C.: The first step for an intelligence service is to be prepared to vigorously study lessons learned. You're doing that. I'm seeing that. You have to be introspective. You have to encourage reflection. You have to encourage, even if it's never published, people to write internally, and to share their perspectives and lessons learned. That's the first step, to recognize that the world is changing and intelligence services have to be far more adaptive. And I'll give you an example. The United States, much to the chagrin and anger, if you will, of some of my former colleagues, don't like the fact that intelligence sharing has been so dramatically changed as a result of the war in Ukraine. In other words, we have declassified in the United States a lot of sensitive intelligence. I think it's brilliant. I think it's inspired. And I think it is an important evolution of information and the use of social media to get ahead of our adversaries. For example,

according to media reports, the United States seemed to know that Russia was going to conduct some kind of act that would be a pretext to suggest that Ukrainians employed chemical weapons. According to the media, the United States seemed to understand that a ruse by Russia was to be implemented. As a consequence, the United States shared that intelligence, so if it happened, everybody knew that it was a Russian disinformation operation. That's staying ahead of the speed of information. And that's just one example. How do we reconcile social media? How do we use social media? Well, the United States, and at least the United Kingdom, because I'm not tracking Polish media, are now publishing and advertising openly, hey, if you're not happy with Putin, reach out to CIA, and here's the number, and here's how you can do it securely. Brits are doing the same thing. We know there are a lot of dissatisfied Russians, both of us, you and I understand that. How do we tap into that? If you can use X (former Twitter) accounts for bad purposes, or malign purposes, you can use social media for good or to benefit security services.

Security professionals have to reconcile everything from 3D printing, cryptocurrency, and all of these new-century dynamics, to quickly come together in order to better understand the threats. Artificial intelligence is another looming problem, and the United States has to do so, along with the world community, and it can't be a U.S. only solution, especially staying ahead of artificial intelligence. I have just participated in a brief conference, where I heard from former senators about the challenges with policy on how to stay ahead of AI. There is no universal policy for artificial intelligence, but we have to work with the international community in ways we never have before. The United States certainly did that with Huawei. I don't know what Poland's use of Huawei was, but I know that media reported that the United States recognized the serious implications of Huawei in China having a 'backdoor' for collecting data, it wasn't heavy-handed, but the United States shared their concerns with partners, and many partners recognized threats to privacy. We have to do the same with artificial intelligence. We have to understand what the risks are, and what the opportunities are, but what are our vulnerabilities, too? And the other thing I want to say is the United States produces unclassified intelligence on the kinds of the threat we're seeing from the world, and we publish that for the public. The Director for National Intelligence publishes

a worldwide threat assessment. These ideas of threats from AI misuse, the idea of global pandemics, maybe more dangerous than COVID, the idea of dissatisfied populations, the idea of not just more far-right extremist or populist views, but also those views that are manipulated by intelligence services, will make more nations vulnerable to anti-government action against them. In other words, there is a trend that is coming into sharper focus that governments are going to be more vulnerable. For example, people believe that the government can't protect them from COVID; the government can't protect them from losing their life savings from hacking. With all of these things and technologies, people being unable to keep up with all the technological change, and artificial intelligence, nations are more vulnerable than ever. So, it's intelligence and security services that are the first line of defense. I'm glad that when I exercised my tradecraft overseas, it was 'old school'. The Russians used the same kind of tradecraft I did. It was universal. And so did Poland. Life was simpler.

The world has changed dramatically because of technology. It is very challenging. But I do have faith, especially when I looked at the people that were in the auditorium today and heard their questions, it's no different when I talk to the FBI and other agencies. In short, I'm confident that this generation will figure it out.

The last question is that you are the Director of the famous International Spy Museum in Washington, are there exhibits directly related to the history of operational activities carried out as part of the war on terror?

Ch. C.: Well, unfortunately, we show the public the consequences of strategic surprise of 9-11 in particular, and it's related to what you said, the exigency and the circumstances of 9-11 changed the United States' focus on counterterrorism. And it forced the interagency to communicate in ways they never did before. Unfortunately, we don't want to wait for a crisis to cause necessary change, but it does. So at the Spy Museum, we talk not just about 9-11, we compare that strategic surprise to Pearl Harbor, and we demonstrate interactives on cyber vulnerabilities, too. We show the public national security decision-making in the decision to launch a raid against Bin Laden. We show briefly how the operation was executed, that's important,

but what's more important to educate the public, is how was that the decision made to launch a raid. And how do you red team-challenge- your own intelligence judgments? And who were those faceless, nameless analysts? How did they do their work long before we executed the operation?

The Spy Museum tells those stories. Also, when you go into our fourth floor, which is why nations spy, our stories include strategic warnings. The Museum does not just focus on jihadists and post-9-11 terrorism, we tell stories about anarchists and militia threats in the United States. The red scare and anarchist fears in 1919, for example. The birth of the FBI came out of J. Edgar Hoover investigating anarchists, right? We address the Oklahoma City attack. The International Spy Museum focuses on a wide array of stories. And of course, one of my favorite and deeply personal stories is 1972 Munich. I was 10 years old when the attacks at the Munich games took place, so you now know how old I was, if you already didn't know. I watched that live. So did 900 million other people across the world. That got my attention as a 10-year-old. That ushered in a whole new era of terrorism, but also slowly shaped into the wave we're still dealing with, which is jihadi-inspired terrorism. The Museum tells all of those narratives at a very macro level. And we have artifacts that highlight those periods in terrorism history. And also, we show the public interrogation through history. And I don't mind saying that we tackled the controversial subject of enhanced interrogation. I won't talk a lot about that here, because I want your readers to come visit and see how we handle that in the Museum.

Can I offer another comment? I want to make another important point. I want to again stress that, I went to the uprising museum here in Warsaw. The story of Polish resistance, the story of tradecraft, and you used the word resilience in the second world war, is an extraordinary model of courage. And I tell anyone that will listen about Polish courage and resilience. It's crucial still to understand the importance of unconventional warfare. We didn't talk a lot about that today. But much of my career was focused on understanding resistance and unconventional warfare. And working with people that studied it and practiced it. So, I believe strongly that Poland is an extraordinary example to study in terms of resilience, resistance and irregular warfare. In light of Russia's malign behavior those lessons are enduring and are worth thinking about.

We also tell a human intelligence story of an individual that was from Denmark and volunteered his services, and was recruited as a spy. His name is Morten Storm. He knew Anwar al-Awlaki, a propagandist for AQ. That's one of the first stories we tell on counter-terrorism. But through the lens of human intelligence. The Museum also, in that same gallery on human intelligence, tells the story of an Israeli Shin Bet officer, and a Palestinian that was associated with Hamas (it is about Mosab Hassan Yousef- editor's note). The Museum shows the dynamics of the clandestine relationship between source and handler. I appreciate how the Museum tells that story, as somebody who's handled sources. The *Green Prince* was a book written about that particular story.

And then the next story on counter-terrorism is about analysis. And how prior to 9-11, mostly women analysts at CIA and elsewhere in the U.S. intelligence community, were tracking Bin Laden, before, during, and after 9-11. And those women talk about some of their analytical tools. We tell that important story. And there are some great interactives. And that transitions into a red-teaming exercise that shows the Bin Laden compound. And shows the public examples of national security decision-making. I've talked about my White House experience working terrorism. There, I wouldn't have been the ultimate decision-maker for the Bin Laden raid. In that case, the President of the United States was the decision maker.

The Museum also compares the dynamics of 9-11 to Pearl Harbor. And the dynamics are almost the same. Everything from mirror imaging to noise versus signals. Here again, we tell that story from the lens of history. As noted already, the Museum transitions to anarchists in places like Washington, D.C. in 1919. We have artifacts from the Oklahoma City federal building attack. And then, lastly, as I already shared my personal recollections of 1972 Munich, we tell that story, too.

The Museum permanent exhibition shows the history of espionage and tradecraft during the Cold War, and how similar some of the things are for providing important context for what we're seeing in Ukraine today. We talked about the idea of resistance and unconventional warfare, and irregular warfare, the Museum has artifacts for those efforts during WW 2, that by the way, Poland practiced and executed so well. It's important to note that we're seeing Ukraine exercises some excellent examples of unconventional warfare

Terrorism – Studies, Analyses, Prevention
2024, no. 5: 423–434

against Russia. Those past lessons must be considered instructional and worth reconsideration as the West must counter the subversive work of Russia.

The International Spy Museum does not take a position. We don't tell people what to think. They decide. And I think that's important. These are really important questions, thank you.

He was talking: Damian Szlachter

Colonel (Ret.) Christopher P. Costa

Retired intelligence officer. He served in the Department of Defense for 34 years, during which he spent 25 years as an intelligence officer with Special Operations Forces (SOF). He was recognized for his sensitive human intelligence work in Afghanistan with two Bronze Stars. After retiring from the military, he continued to serve at the Naval Special Warfare Development Group as a civilian and was later inducted into the United States Special Operations Command Hall of Honor for his lifetime service to US Special Operations. Colonel Costa's most recent role was as the Special Assistant to the President and Senior Director for Counterterrorism at the White House. He is now the Executive Director at the International Spy Museum.