



**Two Air Force F-35 Lightning II aircraft arrive in Lithuania in late February to support NATO's collective defence**

# STRATEGIC PLANNING

**Jawhar Farhat** examines the need for a national security plan in light of the Russian invasion of Ukraine

**T**he establishment and maintenance of a secure society requires a strong, and professional security state. As a result, governments will strive to integrate law enforcement agencies' work and coordinate it to increase impact, focus duties and reduce unnecessary complexity. About the Russian-Ukrainian war, risk analyses are more accountable for assessing data related to introducing a wide range of instability-

related events that are critical to the governments and its various operations which can abuse public security.

The national security plan is a strategy that the highest levels of government sign and promote. That considers the international, regional and domestic contexts to determine what is in a nation's best interests, sets objectives to advance or protect those interests, and then finds innovative ways to use the means at the nation's disposal, or if those aren't available, to generate the means

and resources necessary to implement the strategy at a later date. A national security plan process also entails analysing the costs and risks of a chosen course of action, as well as continuously scanning the environment for changes that could jeopardise your approach. However, there are many variations in this description, but it is an ends-ways-and-means structure that is widely acknowledged in the national security community, even though many people use it in different ways or change it. As a result, we're not simply talking about military strategy, economic growth plan, negotiating strategy or environmental strategy; we're talking about a strategy that considers these factors.

An outward-facing strategy may be concentrated on your country's neighbours or the worldwide environment, whereas an inward-facing strategy is focused on your own country and what's going on internally, as well as the ability to generate funds to ensure that outward-facing plan.

## THE RATIONALE FOR HAVING A NATIONAL SECURITY STRATEGY

On some occasions, a break from the past may be necessary. A change in the worldwide environment, the regional environment, the domestic environment or the individual leader, for example, could all be factors. There are various more reasons for these environmental changes. A country may seek to develop a strategy to create a shared vision of the future to achieve national unity of effort and to prioritise resources.

At the same time, a nation might want a strategy to maintain a strong vibe going, keep a government in place, bring hope or confidence, manage risk, gain access to a system, change a system or tear down the entire system.

Governments may not want to inform their adversary what they are up to in secret. You may not want it written if you have one in your head. Furthermore, governments may not want a strategy, since it will bind them if they tell everyone what they're going to do, and they will lose credibility as senior strategists if they do so. Governments may not want a strategy if public opinion opposes it, if it violates international law or if it fails because they cannot plan, and they may not want a strategy because it allows them as a leader to have a force of their personality, a cult of their personality. Furthermore, it places them in charge, establishing them as the leaders in charge and decision-makers.

## THE MEANS FOR IMPLEMENTING A NATIONAL SECURITY STRATEGY

When we talk about means, we might think of them in three different ways: institutions, people and things. Objects which can be touched or palpable things, is a term we might use to describe them. Treaties, accords, communication resolutions, summits cables, verbal notes and marshes are also included. These are all diplomatic tools that can be used in a variety of ways. When we think of institutions and think tanks that disseminate information, we think of universities and think tanks. The intelligence communities deal with both information and people; they have spokespersons, reporters and analysts.

Newspapers, televisions, radio broadcasts, satellites, intelligence concepts and symbol logos are all examples of things. These are tools for gathering information. On the military side, we can have defence ministries, interior ministries, institutions, regional organisations

and military command. There are also planes, ships, tanks, troops, commanders and police, as well as paramilitary law enforcement.

Furthermore, there are government ministries, the World Bank, the UK Infrastructure Bank, regional economic communities, grants and loans, scholarship help and stock exchanges. As a result, a country has a lot of things, a lot of means and a lot of resources at its disposal. Finally, the art form is figuring out how to put them together over time to achieve the goals that governments set for themselves.

## WHO'S RESPONSIBLE FOR STRATEGY DEVELOPMENT?

From my perspective, everyone handles strategy creation. It's also a reflection of growing democratisation and democracy. So, in a democracy, the planning process appears different from how it is in a country with a powerful leader or a dictatorship. However, servant leadership is one approach to positive strategy creation. It fosters agreement by educating individuals about the nation they serve, the goals they are attempting to achieve and the importance of putting people's interests ahead of the nation's.

## ANY NATIONAL SECURITY POLICY IS A WORK IN PROGRESS THAT MUST BE REGULARLY UPDATED

The triangle of interests, which includes dangers, opportunities and objectives, is used to assist identify some of the key components. Furthermore, as part of the context of assessment, an honest understanding of what the government's national interests are, as well as the risks and opportunities that affect those interests: internal dangers, external threats and opportunities are all factors to consider. Governments can then decide what objectives they need to meet to serve those interests and address risks or opportunities, such as seizing or mitigating them.

Moreover, this aids governments much when they jump ahead to objectives, determining whether these aims are serving their interests and whether they will minimise threats or seize opportunities. Otherwise, if the aim is okay, this is a fantastic aim, but if it's not supporting their interests, then it's not so significant, or it seems like a nice aim, but it will not help them deal with that threat, then it's not so vital. In this situation, they'll need to change their goal to ensure that it's accomplishing that. As a result, after they've proven it, they can go on to the details of their methods and means.

In terms of methods and means, consider economics, intelligence, diplomacy and ties with other neighbouring countries, as well as the United Nations. To summarise, much of this is outside the military's purview, thus it's critical to combine civilian dialogue with those outside the government. Governments can, for example, bring in national security councils and business leaders to get their input, as well as civil society leaders from think tanks and advocacy groups, to get their input and give them some ideas, as well as military and neighbours, so that everyone can be a part of the process.

Government leaders should take visions and turn them into an end-goal means package that can then be implemented by patents. For developing a strategy, decision-makers need a reaction from visionary members and actionable members (military), and then each government needs a leader who can think about how to bring these pieces together, which is why having all of those aspects is important.

## IT'S CRITICAL TO COMBINE CIVILIAN DIALOGUE WITH THOSE OUTSIDE OF THE GOVERNMENT

Then it becomes intimate ties, and it's important to cultivate those interactions not only within services but also between military and civilians. Furthermore, while there are many various sorts of national strategy, they all follow the same core principles: developing an assessment of context; defining interests; defining threats and opportunities; defining ; assessing risks; developing ways and means; and determining costs. When deciding on a strategy, it's necessary to evaluate factors such as feasibility, sustainability, affordability, assumptions, strengths, and weaknesses of your competitors' strategies, continuous evaluation, and measurement of performance, adjustments, and adaptability. To summarise, any national security policy is a work in progress that must be updated and changed regularly.

The Russian cyber threat is not only serious, but it's also unexpected, so policymakers prefer to warn the

world that cyber weapons can be used as weapons and have the same rules that would prohibit or regulate the use of a missile. We've seen in the past that Putin isn't interested in moving on to the second stage of analysis and considering whether he might start using a cyber weapon in a way that violates those rules, something that isn't focused on Ukraine but could, by design or by accident, spread to companies around the world.

We could see a kind of catastrophic set of attacks that would hit indiscriminate companies all over the world if the Russian government didn't inflict billions of dollars in losses in American and European companies during a stage when he wasn't in a kinetic war.

Those attacks might not be obvious, and they might not have a definite goal in mind. As a result, one thing we witnessed from the Colonial Pipeline ransomware targeted attack, which brought the pipeline's activities to a halt for a period. Also, we saw an assault that took use of a Microsoft weakness to prevent anyone from utilising the infected PCs, therefore rendering them worthless.

If that's what indiscriminately takes down any computer using this software that hasn't been patched, we have to consider how disruptive that could be. Therefore, it may not be a targeted attack, but an indiscriminate attack that shuts down systems all around the world.

As a result, the entire cyber community is on high alert right now, with cyber security companies and all of their partners, including those who would normally compete, cooperating to collect as much data as they can or any technical information with any customers who want it, and they're normally attempting to identify the Russians' tactics quickly so that people can patch against them and then share effective skills ●

**Jawhar Farhat** is a certified security management professional (CSMP) Level 6 diploma who graduated with a Master's degree in Military Sciences from Fondouk Jedid Military Academy of Tunisia. He gained his expertise both in his current employment as a Risk Analyst and during his service in the military as a First-Lieutenant. Now, he is assisting security and risk professionals in making an obvious influence on their firms and helping them prevent potential concerns.

**The entire cyber community is on high alert against Russian cyber attacks**



Picture credit: US Dept Defense