Version: 1.2

War Planning Self-Assessment Checklist

Organization Name: _____ **Date: _____**

This checklist is a self-assessment of the risk that a specific regional or global conflict scenario could impact an organization's operations.

The checklist provides an opportunity to pause and think through various steps that your organization could take to prepare for a conflict. Some of these questions may be uncomfortable to address, but better that they be asked in advance, rather than when a conflict occurs.

This assessment should be performed separately for each specific conflict scenario that an organization faces, as the degree of exposure and preparation may be quite different with respect to different scenarios.

Each of the questions on the "Executive Summary of Overall Risk" page map to more granular questions in the "Detailed Risk Assessment" section. It makes sense to answer the "Detailed Risk Assessment" questions first and feed the overall conclusions back up to the "Executive Summary" page.

This list of questions may not be comprehensive of every consideration that is relevant to your organization. It is meant to provoke thinking about this topic, but it may not be exhaustive.

If you have ideas or feedback about the checklist please contact us: info@kopidion.com

Executive Summary of Overall Risk

Conflict Scenario: _____

Enter the potential future conflict scenario you are addressing here. It helps to define a scenario involving a specific geography and set of actors so that likelihood and exposure can be evaluated.

The questions on this page allow you to draw overall conclusions regarding the examined scenario. We suggest that you do not answer these questions now, but do so after completing the three sections of the "Detailed Risk Assessment."

Geopolitical Risk
Summary of Section 1: Estimating the Probability of the Scenario Occurring**.** Please enter estimated values after answering the questions in Section 1 of the Assessment.

	0-2 Years	3-5 Years	6-10 Years
Probability of the scenario occurring	_____%	_____%	_____%

Exposure
Summary of Section 2a-2d: Estimating the Impact of the Scenario on the Organization.
Please complete after answering these questions in Section 2 of the Assessment.

	Direct (Y/N)	Indirect (Y/N)	Collateral (Y/N)
Estimated impact that the scenario would have on our organization (i.e. our exposure)			

	Yes	No
Is our organization likely to be targeted?		

Impacted Areas

Summary of Section 2e: Estimating the Impact of the Scenario on the Organization. If any of the individual answers in Section 2e are "Yes," then the overall answer marked below should be "Yes."

	Yes	No
Direct Operational Impacts		
Third Party		
Infrastructure		
Market		
HR		
Financial		
Regulatory		

Readiness

Summary of Section 3: Is My Organization Prepared for the Conflict Scenario? This Section is designed to assess if your organization has done sufficient planning and preparation in each of the areas below to limit the impact of this scenario on the organization's operations.

Please complete after answering all questions in Section 3 of the Assessment. Mark the average score for each of the areas outlined below. Scores range from 1 to 5. Low scores reflect low preparedness, high scores reflect high levels of preparedness.

	Average Score
Resourcing	
Intelligence & Awareness	
Plans & Policies	
Command & Control	
Human Resources	
Operational Resilience	
Infrastructure/Technical	
Training	
Legal	

Detailed Risk Assessment

Section 1: Geopolitical Risk - Estimating the Probability of the Scenario Occurring

The overall Geopolitical risk should be a rough estimate of the probability that the scenario you are considering will occur within a particular timeframe - short term or long term. **Please rate each question on a 1 to 5 scale, with 1 indicating longer term risk and 5 indicating nearer term risk.**

	1	2	3	4	5
How stable is the current political environment in the region associated with the scenario? Consider historical conflicts, recent uprisings, or ongoing tensions.					
What is the nature of the relationships between the countries involved and their neighboring countries? Include considerations of border disputes, trade conflicts, and diplomatic relations.					
How would you rate the internal political situation of the countries involved? Consider factors like government stability, prevalence of corruption, and the effectiveness of rule of law.					
Has either side in a potential conflict issued any public communications, either officially or through proxies, that threaten military action or retaliation?					
What is the level of military presence and activity in and around the regions where your company operates? Have there been recent changes to military presence or an increase in "training exercises?" Consider both national and foreign military forces, including peacekeeping troops.					
How susceptible is the region to the spillover effects of global geopolitical tensions? Consider factors like global power struggles, economic sanctions, and international alliances.					

Your answers to the above questions will inform your answer to the **Geopolitical Risk** question on the Executive Summary page - Estimated Probability of the Scenario Occurring.

Section 2: Exposure - Estimating the Impact of the Scenario on the Organization

Assessing the impact of a conflict scenario to an organization requires determining the amount of exposure the organization has to the conflict, the likelihood that the organization will become a target, and the possible impacts that the conflict may have on the organization.

These questions are broken down into sections. **The questions can generally be answered on a yes/no basis.** If any of the individual answers are "Yes," then the overall answer marked in the "Executive Summary" page should be "Yes."

A. Does my organization have direct exposure to the conflict?

	Yes	No
My organization has a physical presence in the conflict region.		
My organization has mission critical business functions performed in the conflict region or operational dependencies on our infrastructure in the conflict region.		
My organization has sensitive data in or direct network connectivity with the conflict region.		

B. Does my organization have secondary exposure to the conflict?

	Yes	No
My organization has dependencies on third parties with direct exposure.		

C. Does my organization have collateral exposure to the conflict?

	Yes	No
My organization may experience impactful collateral effects from this conflict (i.e. global DDOS attacks or malware).		

D. Is my organization likely to be targeted?

	Yes	No
My organization may be targeted because it directly supports a side of the conflict or because it provides critical infrastructure services to the region of the conflict.		
My organization may be targeted symbolically because it is perceived to support a side of the conflict.		

Prior to this scenario occurring my organization has been a target for the adversary or has been targeted by other nation state actors (including network compromises).		
Adversaries in the potential conflict zone have probed my organization's infrastructure.		
My organization has capabilities and valuable resources that could advantage one side or the other.		
During the conflict, my legitimate customers may use my organization's infrastructure in ways that enable military operations or make my infrastructure a target.		
My organization has offices or other infrastructure in close physical proximity to sites that may be targeted, such as military sites or facilities.		
During the conflict my organization will take actions that may make my organization a lawful target in the conflict.		
During the conflict my employees may take unsanctioned actions that make my organization a lawful target in the conflict.		
My organization's team members have been approached by suspected agents of the adversary.		

E. How will the conflict Impact my organization?

I. Direct Operational Impacts

	Yes	**No**
My organization has offices and/or operations in the region which may be disrupted, temporarily or permanently, by a conflict.		

II. Third Party Impacts

	Yes	No
My organization or our supply chain are operationally dependent upon third party organizations that operate in the region or who may be impacted for other reasons.		
My organization may face governmental prohibitions on cooperation and trade with the current partners.		
The conflict may result in boycotts or prompt other companies to exit markets, resulting in an impactful loss of access to third parties and infrastructure.		
The government may change or prohibit software applications or services the organization depends on, due to the conflict.		

III. Infrastructural Impacts

	Yes	No
Our offices inside the conflict region would be impacted by disruptions to local infrastructure and services (power, internet, water, sewer, transportation, etc)		
Our infrastructure may experience temporary outages either as a result of direct targeting (such as DDOS attacks) or an indirect result of damage to third party infrastructure that we depend upon (such as telecommunications infrastructure).		
Our infrastructure may be commandeered or repurposed by one of the actors in the conflict.		
State actors may covertly compromise systems and networks in our IT ecosystem.		
Our infrastructure may be destroyed by one of the actors in the conflict.		

IV. Market Impacts

	Yes	No
Customers or activists may organize boycotts against my organization due to this conflict.		
My organization's consumers or customers may be confused about my organization's role in the conflict.		

V. Human Resource Impacts

	Yes	No
Some of my employees are citizens of one of the countries that is party to the conflict.		
My organization may face new employment restrictions and prohibitions that impact operations.		
My organization may face new immigration restrictions that impact operations.		
Team members and their families in the conflict region may be impacted by curfews and internal travel restrictions.		
The organization's team members may be drafted and military reservists called to active duty due to the conflict.		
My organization's employees have close family members in the affected region at physical risk.		
Members of my organization's team and their family members may be arrested by adversary law enforcement or military.		
There is a risk that some employees will become insider threat actors because of this scenario.		
There is a risk that employees may leak sensitive information to one of the combatants.		
It is possible that my organization has a threat actor's agent on the staff already.		

VI. Financial Impacts

	Yes	No
My organization has exposure to financial markets in the conflict region.		

VII. Regulatory Impacts

	Yes	No
My organization may face new taxes or tariffs due to the conflict.		
My organization may face new travel restrictions and prohibitions that impact operations.		
A government will ask for my organization's assistance in support of their side of the conflict.		

Your answers to the above questions will inform your answer to the **Exposure** and **Impacted Area** questions on the Executive Summary page which asks you to estimate the impact the scenario will have on your organization.

Section 3: Readiness - Is My Organization Prepared for the Conflict Scenario?

Various facets of readiness should be assessed. **These questions are best answered on a 1 to 5 scale, with 1 being the lowest level of preparedness and 5 being the highest**, and then each section's scores should be averaged. The averages can be recorded on the "Executive Summary" page.

A. Resourcing

	1	2	3	4	5
My organization has sufficient resources dedicated to the war planning and preparation efforts.					
My organization has a dedicated senior leader who oversees war planning efforts. This individual is held accountable for results and possesses authority to enable desired progress.					
Wartime preparedness is integrated into my organization's performance management systems (e.g. OKRs) to provide appropriate prioritization and executive visibility.					

B. Intelligence & Awareness

	1	2	3	4	5
My organization has sufficient threat intelligence programs and resources that accurately monitor the likelihood of this scenario occurring.					
My organization tracks conflict trends on relevant areas of interest.					
My organization's threat intelligence program has developed intelligence Indicators & Warnings to provide early warning of crisis probability changes.					
My organization participates in national and/or industry sector information sharing networks that communicate threat intelligence and situation updates.					

My organization has reporting mechanisms to keep organizational leadership informed of potential crisis(es), especially regarding increasing probability of conflict.					
My organization is receptive to tracking the probability of war and is receptive of initiatives to support preparedness.					
My organization has a feedback loop that lets employees in the potential conflict zone report on developing situations on the ground.					
My organization directs its intelligence assets with new requirements based on the changing risk environment.					
My threat intelligence team is monitoring current geopolitical crises to develop lessons learned applicable to my organization.					
My organization has members of the team that will monitor social media climate before and during the crisis.					

C. Plans & Policy

	1	**2**	**3**	**4**	**5**
My organization has conducted a tailored risk assessment for this scenario.					
We have a written plan for how the organization will respond in the event that this specific scenario occurs.					
Our plan has tiered, pre-planned response actions, and approving authority to take in the event of increasing likelihood of the scenario occurring.					
Our plans include the scenario of my organization becoming a target.					
Our plans include responding to sanctions and boycotts due to a war.					

We have plans in place to evacuate employees, contractors, and their families from conflict regions in the event of an impending war.					
Our plans consider the possibility of exiting markets in the event of a war.					
Our plans consider the possibility of denying access to products and services from markets.					
We have developed a list of offensive actions and capabilities the company could take in the event of a war as well as criteria covering when and if they would be used.					
Conflict planning is integrated with my organization's existing Risk Management, Crisis Management, Business Continuity Planning, and Cyber Resilience programs.					
My organization's public affairs and marketing teams have strategic communications plans to communicate with customers and the public in the event of a war.					
Our conflict plans have received senior leader approval.					
The existence of the plan has been communicated to appropriate members of my organization.					
My organization's conflict plans are sufficiently secure from compromise by adversaries.					
My organization's conflict plans are reviewed and updated on a regular basis.					

D. Command and Control

	1	**2**	**3**	**4**	**5**
Our conflict plan establishes a clear chain of command. Someone is clearly in charge.					

My organization has resilient alternate means of communication to the affected areas in the event of disrupted primary communications.					
My organization has an established Emergency Operations Center (EOC), or similar, for use during a crisis.					

E. Human Resources

	1	**2**	**3**	**4**	**5**
We regularly conduct background checks of sufficient depth to identify employees with family members in the threat actor country that could be used to coerce cooperation of our employees, especially senior leaders.					
We make job assignment and information access decisions based on susceptibility of employees to foreign coercion due to this scenario.					
We have sufficient internal controls to prevent formerly trusted, but newly generated insider threats from leaking sensitive information, granting access to infrastructure, sabotaging capabilities, and other malicious activities.					
My organization has employees or contractors physically present in the conflict region and may be at physical risk. We know specifically who and where they are.					
My organization tracks international travel of employees to high-risk areas of the planet.					
My organization has written procedures for extracting employees from high-risk regions in the event of an emergency.					

F. Operational Resiliency

	1	2	3	4	5
My organization has reviewed and identified all of the work that is performed by offices in the conflict region and what dependencies different parts of the organization have on that work.					
My organization has reviewed all of our third-party relationships to identify any who have operations or dependencies in the conflict region.					
My organization has the pre-planned ability to sever all operational dependencies upon both organizational and third-party assets located in the conflict region or that are likely allied with the adversary, pivoting any work performed or infrastructure provided within the conflict region to other trusted regions.					
My organization has redundant supply chains in place to cover those that would be disrupted by the conflict.					
My operation inside the conflict region can function independently without HQ contact and third parties outside of the conflict region.					

G. Infrastructure/Technical

	1	2	3	4	5
My organization has assessed the vulnerabilities of our IT infrastructure to attacks that are likely, given the conflict scenario.					
My organization's infrastructure would be resilient in face of a focused attack by the adversary (including sophisticated network intrusions and DDOS).					
My organization has inventoried all IT infrastructure and services within the conflict region as well as those provided by likely allies of the adversary, including services hosted in third party cloud environments.					

We have backups of any data stored in the conflict region. These backups are located outside the conflict region.					
My organization has the technical ability to isolate or disconnect network assets/offices in the conflict region from the rest of our network and understands the impacts of doing so.					
Offices inside the conflict region have independent IT services and infrastructure such that they can operate without connectivity with HQ.					
My organization has established plans and technical capability to pivot to alternative infrastructure such as cloud infrastructure or satellite communication links in the event that physical/terrestrial infrastructure (such as fiber optic links) are damaged, or in the event of a serious cyber attack.					
My organization has redundant (backup) IT infrastructure outside of the conflict region that duplicates capabilities and services provided within the region, which can be activated in the event that systems or networks in the region become unavailable.					
My organization has plans and technical capability to move, wipe, or encrypt sensitive data resident in the conflict region, if necessary, in the event of this scenario.					
My organization has plans and technical capability to wipe or destroy IT infrastructure in the conflict region, if necessary, in the event of this scenario.					
My organization is prepared for an unanticipated network outage in the conflict zone.					
My organization has plans to mitigate the risk of credentials being coerced from captured technicians.					
My organization has procedures and sufficient spare parts to repair physically damaged infrastructure in the conflict region.					

We have plans to communicate with internal and external stakeholders about loss of infrastructure.					

H. Exercises and Training

	1	2	3	4	5
We have recently conducted a Table Top Exercise (TTX), wargame, or some similar activity to develop and refine plans for this conflict scenario.					
My organization provides sufficient training to its employees on how to respond in the event of this, or similar, conflict scenarios.					
My organization's people have received training on media literacy and influence operations in the past year.					
My organization regularly participates in sector- or national-level cybersecurity exercises.					

I. Legal

	1	2	3	4	5
My organization has access to sufficient legal expertise to advise in the event of an armed conflict.					
Our conflict plans have undergone legal review.					
My organization has existing relationships with appropriate government, military, law enforcement officials and potential allied organizations, in advance of the crisis.					

Your answers to the above questions will inform your answer to the **Readiness** questions on the Executive Summary page which asks you to analyze if your organization has done sufficient planning and preparation for this conflict scenario to minimize impact on your organization's operations.

This checklist was developed by Chris Chiras, Greg Conti & Tom Cross.

The content of this document does not necessarily reflect
the opinions of our respective employers.

For comments, questions, or other feedback, please contact: info@kopidion.com