From report “Sub-Threshold Activities, Intentions, & Indicators: Insights for MSSA in the Information Domain”

Author(s)	**Dr Rob Johnson, Steve Langham & Dr Richard Underwood**
Company	**RED Scientific Ltd**

Sub-Threshold Functions: Scope

Overview

The analysis identified 57 separate functions based on empirical cases in the recent past. A function may be undertaken to achieve more than one intent. Functions may also be clustered to support a single, particular intent. Functions can be found across the range of PMESIIL[1] categories.

Invariably, functions of sub-threshold activity are not deployed in isolation. They can be used in parallel or in sequence to create effects. Sequences of functions are not fixed and may be adjusted dynamically as opportunities or resistance arise. Military and non-military functions may be mixed. Information is used as an effector and also as an enabler.

List of Functions:

Political	1 Provocation, violence 2 Influence through financial support to parties 3 Bribery and influence of media 4 Political placements within target establishment 5 Interference in elections 6 Suppression or influence of voters 7 Disputing iconography, memorials, statues and parades 8 Discord: internal decomposition 9 Manipulation of migrants and refugees 10 Political agitation of civil groups (seize power, incite through rallies, preparation, informal diplomacy) 11 Assassination 12 Blackmail 13 Prevention of ceasefires or election monitoring
Military	14 Occupation/state capture by coup de main 15 Sabotage 16 Temporary border threat or violation 17 Military exercise as deception or threat 18 Logistical support to proxies 19 Biological Warfare 20 Impersonation 21 Nuclear threats 22 Unconventional weapons (vs embassy staff) move
Economic	23 Blockade

	24 Manipulation of energy price or supply 25 Energy contracts to buy permanent influence 26 Imposition of food and trade sanctions 27 Limiting access to markets and goods 28 Unfair commercial practice 29 Currency and banking manipulation 30 Economic front organisations
Social	31 Manipulation of historical narratives and identities 32 Sport as nationalism 33 Manipulation of religion, identity, language and culture 34 Grooming elites to serve as spokespersons for malign organisations
Informational	35 Influence through myths and narratives 36 Cyber theft-and-leak 37 Cyber hacking and intelligence operations 38 Mainstream media disinformation and fake news 39 Use of Public Relations (PR) agencies and think tanks, including those in the West 40 Influence for espionage 41 Malware on apps 42 Psychological operations 43 Manipulation of celebrities 44 Bot amplification and division
Infrastructural	45 5G Infrastructure Dominance for Intelligence 46 Electronic warfare 47 BRI, pipelines and debt manipulation 48 Infiltration of Financial Institutions 49 Influence in international institutions
Legal	50 Launching of international court cases 51 Strategic lawsuits against public participation 52 Creating new citizenship to alter politics 53 Creating border disputes 54 Illegal annexations 55 Breaches of LOAC or international law (attacking crowds, kidnapping, airstrikes on civilians, sexual violence, manipulation of prisoners, ethnic cleansing, conditional humanitarian relief). 56 Legal ambiguity 57 Data theft
OTHER	
Footnotes	[1] PMESII refers to Political, Military, Economic, Social/Societal, Informational and Infrastructural factors.