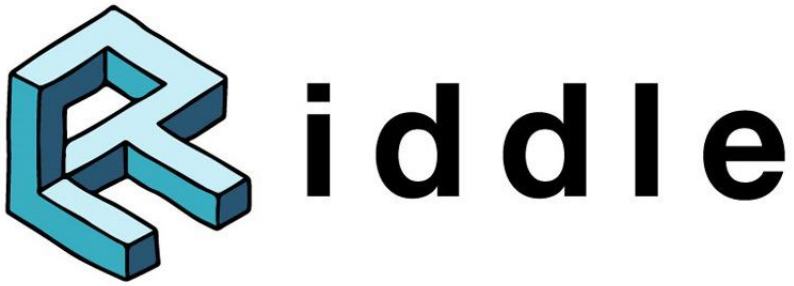

Vulnerability Assessment of Russian Systems Using Chinese Microelectronics

Model*	Type of Weapon / Technology	Manufacturer	Contains China-manufactured microchips?**	Vulnerability to remote access	Technical means of compromise
Platforma-M	Combat UGV	NITI Progress	Likely	Yes	Telemetry hijack, backdoors, malware injection
Nerekhta	Combat UGV	Degtyaryov Plant and Advanced Research Foundation (ARF)	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Soratnik	Combat UGV	Rostec	Likely	Yes	Telemetry hijack, backdoors, malware injection
Kungas	UGV Swarm Concept	Special Engineering Design Bureau	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Scarab	Demining UGV, short-range	CET-1	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Sphera	Demining UGV, short-range	CET-1	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Marker	UGV RDT&E Concept	ARF	Likely	Unknown	Unknown or low-resolution compromise path
Uran-6	Demining UGV, short-range	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Uran-9	Combat UGV	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Uran-14	Firefighting UGV	JSC 766 UPTK (Kalashnikov-Rostec)	Likely	Yes	Telemetry hijack, backdoors, malware injection
Udar	Combat UGV	Rostec	Likely	Yes	Telemetry hijack, backdoors, malware injection
Prohod-1	Heavy Demining UGV	High Precision Weapons JSC	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
Shturm	Heavy UGV for Urban Combat	Uralvagonozavod	Unlikely/Unknown	Unknown	Unknown or low-resolution compromise path
T-14 Armata	Next-Generation MBT (autonomous/semi-autonomous)	Rostec	Likely	Unknown	Unknown or low-resolution compromise path
Nudol system	Ground-based ASAT missile interceptor	JSC Concern VKO Almaz-Antey	Likely	Possible	Targeted EW disruption or spoofing
S-500 system	Air-defence system with potential ASAT	JSC Concern VKO Almaz-Antey	Likely	Possible	Targeted EW disruption or spoofing
Burevestnik (space)	Air-based space launcher	Krasnoarmeysk Scientific Research Institute of Mechanization (KNIIM)	Likely	Unknown	Unknown or low-resolution compromise path

Peresvet	Laser system for satellites/missile blinding	Russian Ministry of Defense	Likely	Unlikely	Vulnerable to optical or electromagnetic countermeasures
Tirada-2	EW system against communication satellites	Central Research Institute of the Ministry of Defense of Russia	Likely	Possible	RF interference spoofing, jamming override
Bylina-MM	EW system for satellite signal disruption	Central Research Institute of the Ministry of Defense of Russia	Likely	Possible	RF interference spoofing, jamming override
Krasukha-4	Radar satellite counter-system	Concern Radio-Electronic Technologies (KRET)	Likely	Possible	RF interference spoofing, jamming override
Divnomorye	Radar satellite counter-system	Concern Radio-Electronic Technologies (KRET)	Likely	Possible	RF interference spoofing, jamming override
Tobol	Satellite protection system	Russian Space Systems (RKS)	Likely	Unknown	Unknown or low-resolution compromise path
Avangard	Hypersonic Glide Vehicle (HGV)	NPO Mashinostroyeniya	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Sarmat	Intercontinental Ballistic Missile (ICBM)	Makeyev Rocket Design Bureau	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Poseidon	Nuclear-Powered UUV	Rubin Design Bureau	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Burevestnik (missile)	Nuclear-Powered Cruise Missile	Novator Design Bureau	Unlikely/Unknown	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Kinzhal	Air-Launched Ballistic Missile	Design Bureau of Machine-Building (KBM)	Likely	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Tsirkon (Zircon)	Hypersonic Cruise Missile	NPO Mashinostroyeniya	Unlikely/Unknown	Possible	Potential firmware backdoors or hardware trojans in COTS components (guidance, nav, comms)
Garpiya-3 (G3)	Unmanned Aerial Vehicle	Unknown	Likely	Yes	Telemetry hijack, backdoors, malware injection
DLE30 engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE55 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE60 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
DLE120 aircraft engines	Aircraft Engine	DLE (China)	Likely	Possible	Engine control manipulation, ECU override
Orlan-10 UAV microchips	UAV Microelectronics	Various (including Chinese suppliers)	Likely	Yes	Telemetry hijack, backdoors, malware injection

* Weapons and technology are composed on the basis of the “Advanced military technology in Russia” report

** Both, military-grade chips and COTS components